## I numeri Naturali, $\mathbb{N}$ .

*Die ganzen Zahlen hat der liebe Gott*
*gemacht, alles andere ist Menschenwerk.*
*(Kronecker)*
*(Dio ha fatto i numeri naturali, tutto il resto è opera dell'uomo)*

### 3.1 Assiomi di Peano e proprietà essenziali dei naturali.

Il primo insieme di numeri che considereremo è quello dei numeri cosiddetti *naturali*, e cioè gli interi positivi più lo zero:

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

Si tratta in un certo senso proprio dei numeri più "naturali" che ci siano, quelli che si usano per contare, ai quali in genere oggi si aggiunge lo zero.

Quelli elencati qua sotto sono gli *assiomi di Peano* (G. Peano, 1858-1932) per i numeri naturali; essi ci mostrano che le nozioni essenziali su cui è costruito $\mathbb{N}$ con tutte le sue proprietà sono quelle di "zero" e "successore" :

1) 0 è un numero naturale.
2) Il successore di ogni numero naturale è un numero naturale.
3) 0 non è successore di alcun numero naturale.
4) Numeri diversi hanno successori diversi.
5) (Principio d'Induzione) Se un insieme di numeri naturali contiene lo zero ed il successore di ogni proprio elemento, allora esso coincide con l'intero insieme dei numeri naturali.

Traduciamo qui di seguito questi assiomi nella simbologia più correntemente usata in matematica (come "$\forall$","$\Rightarrow$" ); scriveremo poi $s(n)$ per indicare il successore del numero $n$ (ad es. $s(3) = 4$ ).

1) $0 \in \mathbb{N}$ ;.
2) $\forall n \in \mathbb{N}$ , $s(n) \in \mathbb{N}$ ;
3) $\forall n \in \mathbb{N}$ , $s(n) \neq 0$ .
4) $\forall\, n, m \in \mathbb{N}$ , $n \neq m \implies s(n) \neq s(m)$ .
5) (**Principio d'Induzione**) Sia $\mathbf{A} \subseteq \mathbb{N}$ un sottoinsieme tale che:
   5.1) $0 \in \mathbf{A}$.
   5.2) Se $n \in \mathbf{A}$ , allora $s(n) \in \mathbf{A}$ , vale a dire: $s(\mathbf{A}) \subseteq \mathbf{A}$.
   Sotto queste ipotesi, necessariamente: $\mathbf{A} = \mathbb{N}$ .

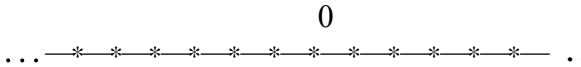
Cerchiamo di vedere come gli assiomi di Peano caratterizzano della struttura di $\mathbb{N}$ , cioè come essi determinano la peculiare struttura di $\mathbb{N}$ , "a catena lineare con elemento iniziale", del tipo "tacche su un bastone":

*—*—*—*—*—*—*—*—*— ...

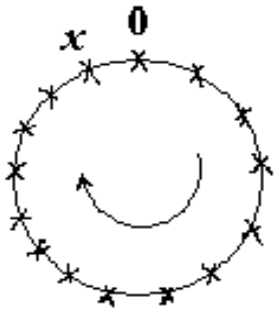
Vediamo singolarmente l'effetto di ogni assioma:

- Il primo assioma ci dice che $\mathbb{N}$ non è l'insieme vuoto; esso contiene almeno lo $0$ (la prima tacca);
- il punto 2) ci dice che "successore" è una funzione $s : \mathbb{N} \to \mathbb{N}$ ("successore" è l'analogo di "scorri da una tacca alla successiva col dito sul bastone")**;**

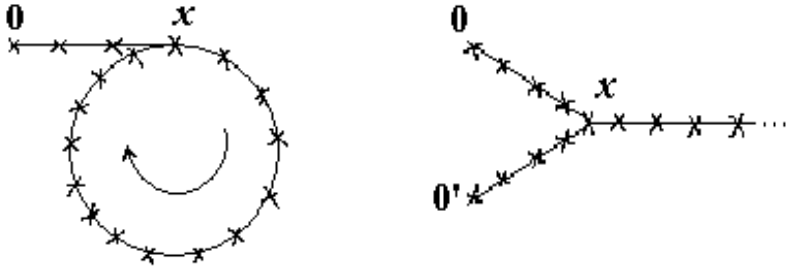
- il terzo assioma identifica la peculiare posizione (potremmo dire di "primo elemento") che caratterizza il numero $0$ in $\mathbb{N}$ , notiamo che esso ha varie conseguenze:
  - per prima cosa ci dice che lo $0$ non è l'unico elemento in $\mathbb{N}$ , in quanto $s(0) \neq 0$ ;
  - inoltre esclude anche una struttura "infinita a destra e a sinistra" (come vedremo sarà la struttura di $\mathbb{Z}$ ) perché qui lo $0$ sarebbe successore di un elemento:




  - infine esclude che la struttura di $\mathbb{N}$ sia "ciclica", come nella figura sotto (dove ci sarebbe un elemento $x$ che ha $0$ come successore ):

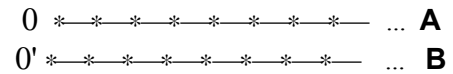



- l'assioma 4) impone che la funzione "successore" porti elementi distinti in elementi distinti. Questo esclude situazioni come le seguenti:




ove due diversi elementi avrebbero l'elemento $x$ come successore.

- Considerando l'ultimo assioma, si ha che esso impedisce ad esempio che $\mathbb{N}$ abbia una struttura "sconnessa" (= fatta di più "pezzi"), come ad esempio se si avesse $\mathbb{N} = \mathbf{A} \cup \mathbf{B}$ :




Vediamo come si può escludere una cosa del genere (che rispetterebbe i primi 4 assiomi); consideriamo l'insieme $\mathbf{A} \subseteq \mathbb{N}$ illustrato sopra, e cioè la "discendenza" dello $0$: tutti quegli elementi che o sono $0$ o si ottengono dallo $0$ applicando ripetutamente la funzione di successore ( nell'immagine sopra $\mathbf{A}$ è la prima riga di tacche).

Ovviamente $0 \in \mathbf{A}$, inoltre se $n \in \mathbf{A}$ , allora anche $s(n) \in \mathbf{A}$, infatti se $n \in \mathbf{A}$ , allora $n$ si può scrivere come: $s(s(s(...(s(0)...)$ e quindi anche $s(n)$ è di questa forma (ha solo una "$s$" in più).

Ma allora il quinto assioma impone che $\mathbf{A} = \mathbb{N}$ , cioè $\mathbb{N}$ è proprio costituito dalla "discendenza" dello $0$, il che ed esclude la presenza di altre "serie di tacche", come $\mathbf{B}$ nella figura.

Si ha che il postulato 5) rende il modello di $\mathbb{N}$ unico, come vedremo rigorosamente più avanti.

Notiamo che il quinto postulato si può "tradurre" utilizzando l'idea del "possedere una proprietà", pensando ad $\mathbf{A}$ come all'insieme costituito dei numeri naturali che possiedono una qualche proprietà $P$; cioè come l'insieme dei naturali $n$ che rendono vero un qualche enunciato aperto del tipo $P(x)$; l'assioma diviene allora:

Sia $P(x)$ un enunciato aperto tale che:
- $P(0)$ è vero ;
- "$\forall n \in \mathbb{N}$ , $P(n) \Rightarrow P(n+1)$" è vero.

  Allora "$\forall n \in \mathbb{N}$ , $P(n)$ " è vero.

Detto "in italiano":

> Sia $P$ una proprietà tale che 0 ha la proprietà $P$ e che se $P$ vale per un numero $n$, allora $P$ vale anche per il successore di $n$; allora $P$ vale per tutti gli $n \in \mathbb{N}$ .

Il quinto è l'assioma più complesso di tutti; per sottolineare l'importanza del Principio di Induzione, notiamo che esso ci permette di dedurre che una proprietà *vale per infiniti elementi* in una singola deduzione.

I cinque assiomi ci mostrano varie cose; ad esempio che per rappresentare i numeri naturali basterebbero (in teoria) solo i simboli " 0" ed "$s$" (a parte le parentesi) , infatti abbiamo che essi sono scrivibili così :

$$0,\ s(0)\ ,\ s(s(0))\ ,\ s(s(s(0)))\ ,\ ...$$

Naturalmente tale modo di scriverli ancora analogo al fare delle tacche su un bastone, sarebbe tutt'altro che pratico, per cui fissiamo l'usuale simbologia:

$$0\ ,\ s(0) = 1\ ,\ s(s(0)) = 2\ ,\ s(s(s(0))) = 3\ ,\ \ldots$$ e così via.

Basandoci sulla nozione di "successore" e sulle sue proprietà, possiamo definire due concetti fondamentali per operare con i numeri naturali: "l'ordine" e l'operazione di "somma".

Per quanto riguarda l'operazione di somma, ricordiamo innanzitutto che un' *operazione* su un insieme $A$ è una funzione $A\times A : \longrightarrow A$ (ove $A\times A$ è il prodotto cartesiano di $A$ per se stesso, cioè l'insieme di tutte le coppie di elementi di $A$); quindi un'operazione è una funzione che ad una coppia di elementi di $A$ associa un altro elemento di $A$ . Ad esempio l'operazione "somma" (che ora andiamo a definire) è una funzione che alla coppia di numeri naturali (2,3) associa il numero 5.

Nel nostro caso l'operazione che definiamo su $\mathbb{N}$ e che chiameremo *somma*, ha simbolo " + " e si definisce, **per ricorrenza**, così:

$$\forall\, m, n \in \mathbb{N}\ ,\ m + 0 = m\ ;\quad m + s(n) = s(m+n)\ .$$

Ad esempio:

$$m+0 = m\ ,\ m+1 = s(m)\ ,\ m+2 = s(m+1) = s(s(m))\ ,\ 3+3 = s(s(s(3))) = 6\ .$$

Ciò vale a dire che si ottiene $m + n = s(s(\ \ldots\ (s(m))))$ applicando ad $m$ la funzione $s$ tante volte quante ce ne vogliono per ottenere $n$ a partire da 0 (cioè $n$ volte).

Perché la definizione "per ricorrenza" è una buona definizione? Cosa ci garantisce che i dati visti sopra definiscono in modo univoco la nostra operazione di somma per tutte le coppie di naturali? Operare e definire così, per ricorrenza è un metodo che si usa continuamente in $\mathbb{N}$ , e lo si può fare grazie al seguente teorema (Dedekind, 1888):

**Teorema di Ricorrenza:** *Sia A un insieme,* $a \in A$ *un suo elemento e* $g : A \to A$ *una funzione. Allora esiste un'unica funzione* $f : \mathbb{N} \to A$ *tale che* $f(0) = a$ *e* $f \circ s = g \circ f$ *(qui s è la funzione successore).*

*Dimostrazione:* Mostriamo prima l'**unicità** della *f*. Supponiamo che ci siano due funzioni $f_1, f_2$ con le proprietà previste; mostriamo, per induzione su *n,* che $f_1(n) = f_2(n)$ per tutti gli *n*. Sappiamo che $f_1(0) = f_2(0)$ , e questo ci dà il primo passo per l'induzione; ora supponiamo che $f_1(n) = f_2(n)$ e vediamo che $f_1(n+1) = f_2(n+1)$ . Usando le ipotesi sulle funzioni, si avrà:

$$f_1(s(n)) = g(f_1(n)) = g(f_2(n)) = f_2(s(n))$$

e ciò conclude il ragionamento.

Per dimostrare l'esistenza della *f*, consideriamo tutti i sottoinsiemi $H \subseteq \mathbb{N} \times A$ tali che:

1) $(0, a) \in H$ ;
2) $\forall n, b$ , se $(n, b) \in H$ , allora $(s(n), g(b)) \in H.$

Poiché $\mathbb{N} \times A$ stesso soddisfa 1) e 2), esistono degli *H* , e tutti contengono (0,*a*); se facciamo l'intersezione di tutti gli *H* otterremo un insieme *D* che ancora soddisfa 1) e 2) e sarà il più piccolo possibile con tali proprietà. Vogliamo usare *D* per definire la *f*, a tal fine dimostriamo che :

(*) $\forall n \in \mathbb{N}, \exists ! b \in A$ such that $(n, b) \in D$ .

Per induzione su *n*; per *n* = 0, $(0, a) \in D$ , e nessun $c \neq a$ sta in *D*, poiché se così fosse, $D - (0, c)$ avrebbe ancora le proprietà 1) e 2) ma sarebbe più piccolo di *D*, il che è impossibile. Quindi se *n*=0, l'unica coppia (*n,b*) in *D* è (*n,a*).

Supponiamo ora che per ogni valore 0,1,2, … ,*n* la proprietà (*) valga e vediamo che vale per *s*(*n*) . Quindi c'è un solo *b* tale che $(n, b) \in D$ e, per la 2), $(s(n), g(b)) \in D.$ Se esistesse un $c \neq g(b)$ tale che $(s(n), c) \in D$ , allora, come per *n*=0, si potrebbe rimuovere $(s(n), c)$ da *D* e ancora varrebbero le 1) e 2), assurdo.

Quindi la (*) è dimostrata, ed ora si può definire $f : \mathbb{N} \to A$ , ove $\forall n \in \mathbb{N}, f(n) = b$ , ove *b* è l'unico elemento per cui $(n, b) \in D$ . Per la proprietà 1), $f(0) = a$ , mentre per la 2) $f(s(n)) = g(f(n))$ , e quindi $f \circ s = g \circ f$ , come volevasi.

**QED**

Il Teorema di ricorrenza ci permette quindi di definire "per ricorrenza" la funzione $f_m : \mathbb{N} \to \mathbb{N}$ (per ogni $\forall m \in \mathbb{N}$ e che scriverò $f_m(n) = m + n$ ) dandone il valore *f*(0) = *m* + 0 = *m* e definendo poi:

$$m + s(n) = f_m(s(n)) = s(f_m(n)) = s(m+n) \ .$$

E quindi ho così definito $m+n$ , $\forall m, n \in \mathbb{N}$ .

Notiamo che la somma ci dà un altro modo di scrivere *s*(*n*), infatti *n*+1 = *s*(*n*) , dato che *n*+1 = *n* + *s*(0) = *s*(*n*+0) = *s*(*n*) .

Per quanto riguarda invece la nozione di **ordine** in $\mathbb{N}$ abbiamo: $\forall n, m \in \mathbb{N}$ , diremo che ***n* è maggiore o uguale ad *m*** (e scriveremo $n \geq m$ ) se $\exists t \in \mathbb{N},$ tale che

$$n = m + t$$

La relazione " $\geq$ ", fra numeri naturali, è quella che chiamiamo una "relazione d'ordine"; non è difficile vedere che essa ha le seguenti proprietà:

1) $\forall$ *n, m* $\in \mathbb{N}$ , se $n \geq m$ , e $m \geq n$ , allora $n = m.$
2) $\forall$ *n, m, s* $\in \mathbb{N}$ , se $n \geq m$ ed $m \geq s$ , allora $n \geq s$ .
3) $\forall n \in \mathbb{N}$ , $n \geq n$ .

La 1) è detta proprietà antisimmetrica; la 2) è invece detta *proprietà transitiva*, mentre la 3) è la proprietà riflessiva.

Valgono poi le seguenti proprietà: la prima ci dice che l'ordine è *totale*, cioè che dati due elementi, essi sono sempre confrontabili, la seconda ci dice che lo 0 è il primo elemento, il *minimo* nell'insieme $\mathbb{N}$ .

4) $\forall\, n, m \in \mathbb{N}$ , o $n \geq m$ , o $m \geq n$ .

5) $\forall\, n \in \mathbb{N}$ , $n \geq 0$

Osserviamo che la definizione di ordine consente un'altra formulazione equivalente del quinto postulato di Peano: il cosiddetto principio del **buon ordinamento**:

**(*) Ogni sottoinsieme non vuoto di $\mathbb{N}$ contiene un minimo elemento.**

**Dimostrazione ( che (*) equivale al principio di induzione).**

Se vale (*), sia $A \subseteq \mathbb{N}$ tale che $0 \in A$ e se $n \in A$ , allora $s(n) \in A$ . Consideriamo $A' = \mathbb{N} - A$ , per dimostrare il principio d'induzione dobbiamo vedere che $A' = \emptyset$ . Se $A' \neq \emptyset$ , per (*) esisterà il minimo elemento $m \in A'$ , e $m \neq 0$ , poiché $0 \in A$ . Allora possiamo considerare il numero $m'$ tale che $m=s(m')$, e $m' \in A$ , ma per ipotesi se $A$ contiene un numero contiene anche il suo successore, quindi $m \in A$ , assurdo.

Se invece assumiamo che valga il principio di induzione, consideriamo $A \subseteq \mathbb{N}$ che non abbia un elemento minimo e mostriamo che $A = \emptyset$ . Mostriamo che nessun $n \in \mathbb{N}$ sta in $A$, per induzione su $n$.

Se $n = 0$ ovviamente non sta in $A$ altrimenti sarebbe il minimo di $A$, quindi $0 \in \mathbb{N} - A$ Se ora $n \in \mathbb{N} - A$ , allora anche $s(n) \in \mathbb{N} - A$ , perché altrimenti $s(n) \in A$ , ma $A$ non conterrebbe elementi minori di $A$ (se no avrebbe un minimo); quindi per il principio d'induzione $\mathbb{N} - A = \mathbb{N}$ e $A = \emptyset$ .

Una conseguenza importante del Teorema di Ricorrenza è **l'unicità di $\mathbb{N}$** :

**Teorema di Unicità di $\mathbb{N}$** : Sia ( $\mathbb{N}'$ , 0', *s*') un'altra terna che soddisfa gli assiomi di Peano. Allora $\mathbb{N}$ e $\mathbb{N}'$ sono canonicamente isomorfi, cioè c'è un'unica biezione $f : \mathbb{N} \to \mathbb{N}'$ , tale che $f(0)=0'$ , e $f \circ s = s' \circ f$ .

**Dimostrazione:** Basta applicare il Teor. di ricorrenza due volte, per trovare le due funzioni $f : \mathbb{N} \to \mathbb{N}'$ ed $f' : \mathbb{N}' \to \mathbb{N}$ e poi altre due volte per vedere che la loro composizione è l'identità.

### 3.2 Le operazioni su $\mathbb{N}$ .

Adesso che abbiamo definito l'operazione di somma, non è difficile verificare che essa gode delle seguenti proprietà:

s1) $\forall\, n, m, t \in \mathbb{N}$ , $n + (m + t) = (n + m) + t$ (proprietà **associativa**).

s2) $\forall\, n \in \mathbb{N}$ , $0 + n = n + 0 = n$ (0 è **elemento neutro** della somma).

s3) $\forall\, n, m \in \mathbb{N}$ , $n + m = m + n$ (proprietà **commutativa**).

Tutte dimostrabile a partire dagli assiomi 1) - 5) e dalla definizione di somma.

**ESERCIZIO**: Dimostrare s1) ed s2).

**Dimostrazione di s3)** . Daremo per dimostrate s1) ed s2). Dimostriamo la s3) per induzione su $n$.

Se $n = 0$ la s3) si riduce alla s2) e siamo a posto.

Se $n = 1$ , dimostriamo che: $1+m = m+1$ per induzione su $m$. Per $m=0$ è vera dalla s2); se è vera per m, avremo che:

$$1+s(m) = 1 +(m+1) = (1+m)+1 = (m+1) + 1 = s(m)+1 .$$

Supponiamo ora che $n + m = m + n$ e vediamo che anche $s(n) + m = m + s(n)$ . Avremo:

$$m + s(n) = s(m+n) = s(n+m) = n + s(m) = n + (m + 1) = n + (1 + m) = (n + 1) + m = s(n) + m .$$

**QED**

Si può poi utilizzare la somma per definire una nuova operazione, la ***moltiplicazione*** (il cui simbolo sarà: "$\times$" oppure "." ). Il processo è simile a quello usato per definire la somma stessa a partire dalla funzione $s$:

$$\forall\, n, m \in \mathbb{N} \text{ , si pone } n \times 0 = 0 \,;\; n \times s(m) = (n \times m) + n .$$

Anche la moltiplicazione gode di proprietà analoghe a quelle della somma:

m1) $\forall\, n, m, t \in \mathbb{N}$ , $n \times (m \times t) = (n \times m) \times t$ (proprietà **associativa**).

m2) $\forall\, n \in \mathbb{N}$ , $n \times 1 = 1 \times n = n$ (1 è **elemento neutro** della moltiplicazione).

m3) $\forall\, n, m \in \mathbb{N}$ , $n \times m = m \times n$ (proprietà **commutativa**).

Ed infine c'è una proprietà che lega moltiplicazione e somma:

sm) $\forall\, n, m, t \in \mathbb{N}$ , $n \times (m + t) = (n \times m) + (n \times t)$ (proprietà **distributiva del prodotto sulla somma**).

Procedendo ancora in modo analogo si può definire su $\mathbb{N}$ , l'operazione di *elevazione a potenza* :

$\forall\, n, m \in \mathbb{N}$ , se $m \neq 0$, si pone $m^0 = 1$ *ed* $m^{s(n)} = m \times m^n$ ; se $m=0$ *e* $n \neq 0$, si pone invece $0^n = 0$ .

Notiamo che non è definito $0^0$ . Questa volta però non abbiamo proprietà analoghe alle precedenti (per esempio questa operazione non è né associativa né commutativa, ad esempio: $3^2 \neq 2^3$) .

Proprietà notevoli della elevazione a potenza sono:

p1) $\forall\, n, m, t \in \mathbb{N}$ , $(m,t) ed (n,t) \neq (0,0)$, $(n \times m)^t = n^t \times m^t$ .

p2) $\forall\, n, m, t \in \mathbb{N}$ , $(m,n) ed (n,t) \neq (0,0)$, $n^{(m+t)} = n^m \times n^t$ .

p3) $\forall\, n, m, t \in \mathbb{N}$ , $(m,n) ed (n,t) \neq (0,0)$, $n^{(m \times t)} = (n^m)^t$ .

Esempi: $5^{11} = 5^{(4+7)} = 5^4 \times 5^7$ ; $3^{(2 \times 2)} = (3^2)^2 = 9^2 = 81$ .

Notiamo che non ha senso cercare di "interpretare" la definizione $m^0 = 1$ come "moltiplicare $n$ per se stesso 0 volte mi dà 1", moltiplicare per sé 0 volte non ha senso; il definire $m^0 = 1$ è un artificio che poniamo per avere l'elevazione a potenza, il cui significato intuitivo è $m^n$ = "moltiplicare $m$ per se stesso $n$ volte", anche nel caso $n$=0, conservando tutte le "buone proprietà" delle potenze.

Questo è un modo di procedere generale in matematica, come vedremo nelle prossime sezioni: si estendono le strutture che si hanno, cercando di salvaguardare le loro proprietà, e passando da una definizione "naturale" (come "elevare a

potenza ennesima = moltiplicare per se stesso $n$ volte"), ad una più "artificiale", meno intuitiva (come $n^0 = 1$), ma che è coerente con la struttura e le proprietà presenti, ampliandole a casi nuovi).

Sottolineiamo che resta invece privo di senso elevare 0 alla 0: il simbolo $0^0$ non rappresenta nessun numero (intuitivamente: abbiamo che ogni numero elevato alla 0 dà 1, mentre 0 elevato ad una qualsiasi potenza dà 0; comunque definissimo $0^0$ contravverremmo almeno ad una di queste proprietà).

A partire da somma e moltiplicazione, si possono definire le loro *operazioni inverse*: la *sottrazione* e la *divisione*, che però non saranno definite per tutte le coppie di numeri naturali, cioè esse risulteranno operazioni parziali su $\mathbb{N}$ (oppure si può dire che $\mathbb{N}$ non è *chiuso* rispetto ad esse). Vediamole:

**Definizione:** $\forall\, n, m \in \mathbb{N}$, si dice $n - m$ quel numero naturale $x$, <u>se esiste</u>, che sommato ad $m$ dà $n$. Cioè :

$$n - m = x \text{ se } n = m + x .$$

E' immediato constatare che un tale numero $x$ esiste se e solo se $n \geq m$ (cioè se $n$ è maggiore o uguale a $m$), quindi l'operazione di sottrazione è eseguibile solo sulle coppie $n, m$ tali che $n \geq m$, e non su tutto $\mathbb{N}$.

In modo analogo alla sottrazione si definisce la divisione:

**Definizione:** $\forall\, n, m \in \mathbb{N}$, si dice $n : m$ quel numero naturale $x$, <u>se esiste ed è unico</u>, che moltiplicato per $m$ dà $n$. Cioè : $n : m = x$ se $n = m \times x$.

Anche per la divisione è immediato constatare che $x$ non esiste sempre, ma se e solo se $n$ è un multiplo di $m$ (cioè se $\exists\, k \in \mathbb{N}$, tale che $n = km$), quindi l'operazione di divisione è eseguibile solo sulle coppie $n, m$ tali che $n = km$, e si può notare che **non si potrà mai dividere per 0**, infatti per avere ad esempio $8 : 0 = x$ si dovrebbe avere $8 = 0 \times x$, il che è falso qualunque sia $x$.

Non si può neanche fare $0 : 0$ in quanto tale operazione risulterebbe *indeterminata*, poiché per ogni naturale $x$ si ha: $0 = 0 \times x$ (cioè $x$ non sarebbe unico), mentre nella definizione si chiede che $x$ esista e **sia unico**.

Le operazioni appena definite danno luogo a proprietà delle potenze analoghe alle p1) e p2):

p4) $\forall\, n, m, t \in \mathbb{N}$, $(n : m)^t = n^t : m^t$ .

p5) $\forall\, n, m, t \in \mathbb{N}$, $n^m : n^t = n^{(m-t)}$.

**3.3 Utilizzo delle potenze per la rappresentazione dei numeri .**

Le potenze sono in effetti essenziali per rappresentare i numeri naturali: il nostro sistema per scrivere i numeri e compiere le operazioni con essi si basa (come abbiamo notato nella parte storica) proprio sulle potenze, ed in particolare sulle potenze del dieci; quando scriviamo 213, 4385 o 765434 quello che ciò significa è:

$$213 = 2.10^2 + 1.10^1 + 3.10^0 ; \quad 4385 = 4.10^3 + 3.10^2 + 8.10^1 + 5.10^0 ;$$
$$765444 = 7.10^5 + 6.10^4 + 5.10^3 + 4.10^2 + 3.10^1 + 4.10^0$$

cioè le cifre che scriviamo rappresentano le quantità, rispettivamente, di unità, decine, centinaia, migliaia, ecc. di cui è composto il numero, e quindi esprimiamo ogni numero come somma di multipli di potenze del dieci.

Naturalmente questa scelta è puramente arbitraria (la sua origine storica è senza dubbio il fatto che possediamo dieci dita delle mani); se volessimo esprimere i numeri in base otto, useremmo solo otto cifre; scrivendole ad esempio: **0, 1, 2, 3, 4, 5,**

**6, 7**. In questo caso il simbolo **10** rappresenterebbe il numero otto, mentre **100** rappresenterebbe il numero sessantaquattro, perché la cifra più a destra rappresenta le unità, la seconda le "ottavine", la terza le "sessantaquattrine" e così via; vediamo qualche esempio di "traduzione" da base otto in usuale base dieci:

$$\mathbf{32} = 3.8^1 + 2.8^0 = 3.8 + 2 = 26 \quad ; \qquad \mathbf{145} = 1.8^2 + 4.8^1 + 5.8^0 = 64 + 32 + 5 = 101$$

Se invece volessimo usare una base più grande di dieci, ad esempio dodici, avremmo bisogno di più cifre, come: **0,1,2,3,4,5,6,7,8,9,a,b** ove **a** = dieci, e **b** = undici; in questo sistema con il simbolo **10** si rappresenterebbe il numero dodici, mentre **100** varrebbe $12^2 = 144$. Qualche altro esempio:

$$\mathbf{23} = 2.12^1 + 3.12^0 = 27\,;\ \mathbf{34b} = 3.12^2 + 4.12^1 + 11.12^0 = 3.144 + 4.12 + 11 = 491.$$

Come saprete, la base più usata, a parte il dieci, è la base 2 (in informatica, nel linguaggio dei computer) in quanto in questa base appaiono solo due simboli: **0, 1** e quindi ogni numero è scritto con una stringa di **0** ed **1**, che rappresentano le potenze del due, ad esempio:

$$45 = 32 + 8 + 4 + 1 = 1.2^5 + 0.2^4 + 1.2^3 + 1.2^2 + 0.2^1 + 1.2^0 = \mathbf{101101};\ \mathbf{1001} = 2^3 + 1 = 9\ .$$

La base due è quella usata dai computer, in quanto in tale base ogni numero può essere rappresentato da una stringa di interruttori, la cui situazione "acceso/spento" rappresenta **0** od **1**, ed è possibile, tramite semplici circuiti, automatizzare somme, moltiplicazioni e così via.

### 3.4 Numeri primi e applicazioni (MCD, mcm).

Vediamo adesso un altro modo in cui si usano le potenze per rappresentare i numeri naturali. Chiediamoci un po', rispetto alle due operazioni di somma e prodotto in $\mathbb{N}$, quali siano i "mattoni fondamentali", i "generatori", cioè i numeri con i quali , attraverso l'operazione, si ottengono tutti gli altri.

Per la somma la situazione è molto semplice: bastano 0 ed 1; lo 0 per generare lo zero stesso, mentre tutti gli altri numeri si ottengono con somme del tipo 1+1+1+1+...+1, quindi i generatori sono solo questi due.

Qual'è la situazione con il prodotto? Dovremo ancora usare 0 ed 1, ma questi generano solo se stessi, quindi dovremo considerare anche il 2, poi il 3, il 4 no in quanto è $2\times2$, poi il 5, il 6 no (= $2\times3$), il 7 sì, l'8 no, il 9 no, il 10 no, ma l'11 si, ... e così via. In sostanza, quali sono i numeri che dobbiamo per forza mettere in questo insieme di generatori?

Sono tutti quelli che non possiamo ottenere moltiplicandone dei precedenti, cioè i numeri che hanno solo due divisori: 1 e sé stessi. Questi numeri sono detti *primi* (per essere più precisi, si conviene di chiamare numeri primi i numeri divisibili solo per 1 e per se stessi a partire dal 2, cioè 1 **non** è considerato un numero primo (non è necessario per generare altri numeri oltre a sé e non ha 2 divisori ma uno solo).

Quindi con i numeri primi si genera (moltiplicandoli) ogni altro numero, ma...

**Quanti sono i numeri primi?**

Sono infiniti o ne esiste solo un numero finito? Se guardiamo ai primi presenti fra i numeri fino a quaranta, ne troviamo 12 :

$$\{\ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37\ \}.$$

Qual è la situazione dopo? I primi si diradano sempre di più fino a scomparire (notate che ce ne sono otto fra i primi venti numeri, e solo quattro nella seconda ventina), o continuiamo a trovarne sempre, per quanto si vada avanti nella successione dei numeri naturali? La risposta a questa domanda è stata data molti secoli fa, e la troviamo negli *Elementi* di Euclide (circa 300 A.C.):

**Teorema:** *Esistono infiniti numeri primi.*

*Dimostrazione:* Supponiamo per assurdo che i numeri primi siano una quantità finita:

$$\{ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots , p\}$$

ove $p$ sia quindi il più grande numero primo esistente. Consideriamo allora il numero $q$ formato moltiplicando tutti i numeri primi e poi aggiungendo 1:

$$q = 2\times3\times5\times7\times11\times13\times17\times19\times23\times29\times\ldots\times p + 1 ;$$

notiamo che il numero $q$ numero non può essere primo in quanto è più grande di $p$, ma non è neanche divisibile per nessuno dei numeri primi, perché è facile vedere che diviso per ciascuno di essi dà resto = 1 (infatti la parte fra parentesi è divisibile per ogni numero primo, essendone un multiplo), quindi siamo arrivati ad una contraddizione:

- $q$ non è divisibile per altri numeri diversi da lui e da 1, quindi dovrebbe essere primo,
- $q$ non può essere primo in quanto è più grande di $p$.

Perciò l'insieme dei numeri primi non può essere finito perché supporlo tale porta ad una contraddizione.

**Q. E. D.**

Questo teorema è forse il più antico esempio di una dimostrazione rigorosa che riguarda direttamente l'infinito, cioè la dimostrazione che un dato insieme non può essere finito.

Per trovare quali sono i numeri primi minori di un certo numero dato, ad esempio tutti i primi minori di 100, c'è un metodo lungo ma efficace, detto il "crivello di Eratostene", dal nome del matematico greco (200 a.C.) che lo ha inventato. Si procede così: si scrivono tutti i numeri da due a 100, poi si cancellano tutti i multipli del 2 (non il due), poi si lascia il 3 e si cancellano tutti i suoi multipli. Il primo numero che resta sarà il cinque: lo lasciamo ed eliminiamo i suoi multipli, poi ripetiamo la cosa con il sette e così via. Alla fine avremo tolto tutti i numeri *composti* (= non primi), e quelli rimasti sono i numeri primi cercati. Può sembrare un metodo molto lento, ma in effetti i numeri primi sfidano tuttora la nostra conoscenza: non esiste un metodo per determinare facilmente se un dato numero è primo o no : si può solo cercare di vedere se è divisibile per numeri più piccoli, e questo talvolta può essere un lavoro molto lungo; considerate per esempio il numero 481477: è primo? No, si ha $481477 = 467 \times 1031$ , e questi due numeri sono primi. Per trovare questi due divisori dovremmo fare un gran numero di prove, e purtroppo non esistono semplici scorciatoie.

Come dicevamo prima, l'importanza dei numeri primi è dovuta al fatto che tutti gli altri si ottengono come moltiplicazione di essi, e la cosa più importante è che vale il seguente:

## Teorema Fondamentale dell'Aritmetica:

*Ogni numero naturale maggiore di* 1 *o è un numero primo o si può esprimere come prodotto di numeri primi. Tale rappresentazione è unica, se si prescinde dall'ordine in cui compaiono i fattori.*

**Dimostrazione.**

**Esistenza:** Dalla definizione di numero primo si deduce che ogni numero maggiore o uguale a 2 o è un numero primo oppure ha un divisore che è un numero primo. Questo fatto si può dimostrare per induzione:

- $n = 2$ è primo, quindi soddisfa quanto enunciato.
- Supponendo vero l'enunciato per tutti i numeri da 2 a $n$, dimostriamo che vale anche per $n$+1. Per $n$+1 ci sono due possibilità: o esso è primo oppure è divisibile per un numero $a$ compreso tra 2 e $n$. Nel caso in cui $n$+1 sia divisibile per $a$ sappiamo per ipotesi induttiva che o $a$ è primo oppure $a$ ha un divisore primo $p$. In quest'ultimo caso $p$ è anche un divisore di $n$+1. In ogni caso dunque o $n$+1 è primo o è divisibile per un primo.

La dimostrazione dell'esistenza della fattorizzazione per ogni numero procede ancora per induzione:

- $n = 2$ è primo e dunque è già banalmente fattorizzato.
- Supponiamo vera l'esistenza di una fattorizzazione per tutti i naturali compresi tra 2 e $n$ e dimostriamola vera anche per $n$+1. Considerando $n$+1, abbiamo due casi: $n$+1 è primo (e quindi è già fattorizzato) oppure $n$+1 è divisibile per un primo $p$ (come dimostrato nella prima parte); in quest'ultimo caso il numero $m = (n+1)/p$ è minore di $n$+1, e quindi

verifica l'ipotesi induttiva, ovvero esiste una fattorizzazione di *m*. Ma allora *n*+1 = *mp* cioè *n*+1 è fattorizzabile (è il prodotto della fattorizzazione di *m* per *p*).

Quindi l'esistenza di una fattorizzazione è dimostrata per ogni numero naturale *n*.

**Unicità:** Dimostriamo che se un numero ammette una fattorizzazione in numeri primi questa è unica.

Si procede **per assurdo**: supponiamo che esistano dei numeri scomponibili in fattori primi in più di un modo, e sia *m* il più piccolo (che esiste per il principio del buon ordinamento). Innanzitutto si dimostra che, date due fattorizzazioni di *m*, i numeri primi che si presentano nella prima fattorizzazione sono tutti distinti da quelli della seconda fattorizzazione. Siano infatti (1) e (2) le due diverse fattorizzazioni di *m:*

(1) $m = p_1 p_2 \dots p_s$

(2) $m = q_1 q_2 \dots q_t$

dove i $p_i$ e i $q_j$ sono primi ma differenti tra loro, ovvero $\forall i, j : p_i \neq q_j$ (se ci fosse un fattore identico $p_h = q_k$ potremmo ricondurci al caso indicato dividendo *m* per tale fattore e ottenendo un numero $m' < m$ che avrebbe anch'esso due fattorizzazioni distinte). Notiamo che all'interno di ogni fattorizzazione ci possono comunque essere fattori ripetuti: ad esempio, 100 = 2×2×5×5.

A questo punto sappiamo che $p_1$ è diverso da $q_1$ ; senza perdita di generalità possiamo supporre che $p_1 < q_1$ . Poniamo allora

(3) $n = (q_1 - p_1) q_2 \dots q_t$

ed evidentemente abbiamo che $n < m$ . Dimostriamo ora che *n* ammette almeno due fattorizzazioni distinte.

Iniziamo considerando il primo fattore di *n* , $q_1 - p_1$ . Esso può essere primo o meno; nel caso non lo fosse lo fattorizzeremo e la nuova fattorizzazione di *n* così ottenuta non ammetterebbe $p_1$ tra i suoi fattori. Infatti, per la prima parte della dimostrazione sappiamo che $p_1$ è diverso da $q_2 q_3 \cdots q_t$ e quindi non può comparire nella eventuale fattorizzazione di $q_1 - p_1$ , poiché se ciò accadesse significherebbe che $q_1 - p_1 = p_1 u$ e quindi $q_1 = p_1 (u+1)$ il che non è possibile e quindi abbiamo dimostrato che $q_1 - p_1$ è primo. Dalla (3) abbiamo adesso:

(4) $n = (q_1 - p_1) q_2 \dots q_t = q_1 q_2 \dots q_t - p_1 q_2 \dots q_t = m - p_1 q_2 \dots q_t = p_1 (p_2 \dots p_s - q_2 \dots q_t)$

Abbiamo così ottenuto (qualsiasi sia la fattorizzazione di $(p_2 \dots p_s - q_2 \dots q_t)$ ) una fattorizzazione di *n* che ha $p_1$ come fattore e quindi è diversa dalla fattorizzazione in (3), contro l'ipotesi che m sia il più piccolo intero con fattorizzazioni prime distinte.

La scomposizione in fattori primi è il metodo più efficace per studiare multipli e sottomultipli dei numeri naturali, in particolare per determinare il *minimo comune multiplo* (mcm) ed il *massimo comune divisore* (MCD) di due numeri dati . Ad esempio, consideriamo i numeri 12 e 18; scriviamone i multipli e sottomultipli:

1 2 3 4 6 **12** 24 36 48 60 72 84 96 108 120 132
1 2 3 6 9 **18** 36 54 72 90 108 126 144 162 180

Ci sono vari divisori, {1, 2, 3, 6}, e multipli {36, 72, 108,...} comuni ai due numeri; tra tutti i più significativi sono appunto il massimo fra i divisori comuni, in questo caso il 6, ed il minimo fra i multipli comuni, qui il 36. Scriveremo allora: MCD(12,18) = 6, mcm(12,18) = 36 .

Come si fa in generale a trovare MCD ed mcm di due numeri?

Per trovare il ***MCD si dovranno prendere tutti i fattori primi comuni ai due numeri, presi col minimo esponente con cui appaiono nelle due fattorizzazioni . Se non ci cono fattori comuni il MCD è pari ad 1.***

Nel caso appena visto avevamo: $12 = 2^2.3$ e $18 = 2.3^2$; e quindi prenderemo $2^1.3^1 = 6$.

I fattori da considerare per determinare il MCD sono solo quelli comuni, in quanto il MCD deve essere un **divisore comune** per i due numeri, quindi i suoi fattori primi devono apparire anche nei due numeri; tali fattori vanno presi con minimo esponente con cui compaiono perché solo così saranno sottomultipli di entrambi i numeri.

Per il ***mcm dovremo prendere tutti i fattori primi comuni e non comuni con il massimo esponente con cui appaiono nelle due fattorizzazioni.***

Sempre nel caso precedente si ha: $2^2.3^2 = 36$ .

Per formare il mcm dovremo considerare tutti i fattori primi che appaiono nei due numeri perché il mcm deve essere un multiplo di entrambi; per la stessa ragione gli esponenti dovranno essere i più grandi fra quelli che appaiono.

**ESEMPIO:** Calcoliamo il MCD(35,98). Come prima cosa eseguiamo la scomposizione in fattori primi dei due numeri:

| 35 | 5 |
|---|---|
| 7 | 7 |
| 1 | |

| 98 | 2 |
|---|---|
| 49 | 7 |
| 7 | 7 |
| 1 | |

quindi $35 = 5.7$ ; $98 = 2.\ 7^2$ . Allora avremo che MCD(35,98) = 7 (unico fattor comune, con minimo esponente). Se vorremo il mcm(35, 98) avremo: $2.5.7^2 = 490$.

**Osservazione.** I metodi appena visti per la ricerca di MCD e di mcm presentano il problema che per numeri grandi la scomposizione in fattori primi può essere piuttosto difficoltosa. Vediamo un metodo diverso (detto *algoritmo di Euclide*) per trovare il MCD di due numeri $a$, $b$. Supponiamo che sia $a > b$ ; è facile notare che ogni divisore comune di $a$ e $b$ è anche un divisore comune di $a - b$ e $b$ , perciò si avrà che

$$\mathrm{MCD}(a, b) = \mathrm{MCD}(a\text{-}b, b) .$$

quindi si può ripetere il procedimento di sostituire il numero più grande con la differenza fra i due, finché non si arrivi a due numeri uguali, il cui valore sarà il MCD cercato.

Ad esempio: MCD(1679,782) = MCD(897,782) = MCD(782,115) = MCD(667,115) = MCD(552,115) = MCD(437,115) = MCD(332,115) = MCD(207,115) = MCD(115,92) = MCD(92,23) = MCD(69,23) = MCD(46,23) = MCD(23,23) = 23.

Questo metodo è quello più adatto ai computer per calcolare il MCD: un computer è molto più veloce a calcolare somme e sottrazioni che a fare moltiplicazioni o divisioni. Nel nostro caso si può sveltire la procedura effettuando la divisione con resto: $a = qb+r$ (vedi il capitolo sugli interi), e quindi ricavare: MCD($a,b$) = MCD($a\text{-}qb, r$) , che equivale a sottrarre $b$ $q$ volte da $a$.

E per trovare il mcm ? Una vota trovato il MCD è semplice: basta moltiplicare i due numeri e dividere il risultato per il MCD:

$$\mathrm{mcm}\ (a,b) = \frac{a \times b}{\mathrm{MCD}(a,b)} .$$

Ad esempio: Per calcolare il mcm(12,18) eseguiamo il prodotto $12.18 = 216$ ; poi sappiamo che MCD(12,18) = 6, e eseguiamo la divisione $216 : 6 = 36$ che è il mcm(12,18).

Come mai questa regola funziona? Perché se abbiamo MCD($a$, $b$) = $k$ , allora si avrà: $a = a'.k$ , $b = b'.k$ (ove $a'$ e $b'$ non hanno fattori comuni), e quindi $a.b = a'.b'.k^2$ , e $a.b : k = a'.b'.k$ , che è multiplo sia di $a$ che di $b$ ($a'.b'.k = a'.b = a.b'$), ed è il minimo multiplo comune, in quanto $a'$ e $b'$ non hanno fattori comuni.

### 3.5 Successioni, Progressioni.

Come ultimo argomento di questo capitolo tratteremo le successioni di numeri naturali, e cioè sequenze (infinite) come:

1, 3, 5, 7, 9 , 11, 13, 15, 17,... ; oppure 5, 15, 25, 35, 45, 55, ...

Le successioni sono utilizzate in vari casi per descrivere l'evoluzione di fenomeni naturali, ad esempio il numero dei membri di una popolazione di cellule giorno dopo giorno, oppure di una mandria anno dopo anno, o la quantità, rilevata ad intervalli regolari, di un elemento radioattivo che decade.

Scriveremo gli elementi della successione come: $S(1)$, $S(2)$, $S(3)$,…. e cioè $S(1)$ è il primo elemento della successione, $S(2)$ il secondo e così via. Essenzialmente una successione è quindi data da una funzione

$S$: $\mathbb{N} - \{0\} \longrightarrow \mathbb{N}$ ,

e può essere assegnata in due modi: *direttamente* o *per ricorrenza*.

Nel nostro primo esempio, la successione dei numeri dispari, l'assegnazione *diretta* della successione si dà dando la legge:

$$S(n) = 2(n\text{-}1)+1 ;$$

che ci dice direttamente come scrivere l'ennesimo elemento della successione, quindi questa ci dice che il primo elemento della successione, $S(1)$, è $2.0+1 = 1$; poi abbiamo $S(2) = 2.1+1 = 3$, e così via.

Invece dare una successione *per ricorrenza* significa darne il primo elemento ed una regola con la quale, dato un elemento, si ricava il successivo. La possibilità di fare ciò e la garanzia che così la successione resti ben definita ci è data dal Teorema di Ricorrenza visto sopra. Nello stesso esempio, dovremmo assegnare:

$$S(1) = 1 \text{ e } S(n+1) = S(n) + 2,$$

cosicché ci ricaveremmo che $S(2) = S(1) + 2 = 3$ ; $S(3) = S(2) + 2 = 3+2 = 5$ , e così via. La legge ci dice che l'elemento di posto $n+1$ si ricava da quello di posto $n$ sommandogli 2.

Spesso si preferisce indicare gli elementi della successione con $n_1, n_2, n_3, n_4,...$ invece di usare $S(1)$, $S(2)$, $S(3)$, $S(4)$, ...

Il primo tipo di successioni che vedremo sono le *progressioni aritmetiche* , e cioè le successioni in cui ogni elemento si ricava aggiungendo una quantità fissa a quello precedente. Tale quantità viene detta *ragione* della progressione.

Ad esempio sono progressioni aritmetiche le seguenti:

2, 4, 6, 8, 10, ... ; 3, 8, 13, 18, 23, 28, ... ; 17, 29, 41, 53, 65, ... ;

la prima ha ragione 2, la seconda 5 e la terza 12. Date per ricorrenza, queste tre successioni si esprimono nel seguente modo:

$$S(1) = 2 , S(n+1) = S(n) + 2 \ ; \ S(1) = 3 , \ S(n+1) = S(n) + 5 ;$$
$$S(1) = 17 \text{ e } S(n+1) = S(n) + 12.$$

In generale, una progressione aritmetica di ragione $k$, del tipo { $n_1$, $n_2 = n_1 + k$, $n_3 = n_1 + 2k$ , ... }, data per ricorrenza si esprime come:

$$S(1) = n_1, S(n+1) = S(n) + k \ ;$$

mentre data direttamente è :

$$S(n) = S(1) + (n\text{-}1).k$$

in quanto $S(n)$ si ottiene in $n$-1 passi a partire da $S(1)$, aggiungendo ogni volta la ragione $k$ .

Un esempio di progressione aritmetica è quello dello stipendio mensile di un lavoratore che abbia uno scatto annuale fisso di 45 euro. Se lo stipendio iniziale è di £ 1.200 Euro, la successione determinata dagli stipendi mensili, anno dopo anno, sarà:

1.200 , 1.245 , 1.290 , 1.335 , 1.380, 1.425, …

I dati che determinano la successione sono: $S(1) = 1.200$ , $S(n+1) = S(n) + 45$ , mentre la legge diretta è: $S(n) = 1.200 + (n - 1).45$.

Vediamo adesso un altro tipo di progressioni: la *progressioni geometriche.* Esempi di progressioni geometriche sono le seguenti successioni:

1, 2, 4, 8, 16, 32, ... oppure 2, 6, 18, 54, 162, ... o 10, 500, 25000, 125000, ...

in questi casi, ogni termine si ottiene da quello precedente *moltiplicando* per una costante fissa, detta ancora *ragione* della progressione geometrica. Se diamo le tre successioni qui sopra per ricorrenza, avremo:

$$S(1) = 1 \text{ , } S(n+1) = 2.S(n) \text{ ; } S(1) = 2 \text{ , } S(n+1) = 3.S(n) \text{ ;}$$

$$S(1) = 10 \text{ e } S(n+1) = 50.S(n) \text{ .}$$

In generale, una progressione geometrica di ragione $k$, del tipo:

$$\{ n_1, \; n_2 = kn_1, \; n_3 = k^2.n_1 \text{ , ... } \},$$

data per ricorrenza si esprime come:

$$S(1) = n_1 \text{ , } S(n+1) = k.S(n) \text{ ;}$$

mentre data direttamente è :

$$S(n) = k^{(n-1)}.S(1)$$

in quanto $S(n)$ si ottiene in ($n$-1) passi a partire da $S(1)$, moltiplicando ogni volta per la ragione $k$ .

L'ultima formula spiega perché un fenomeno descritto da una progressione geometrica si dice che abbia una *crescita esponenziale* .

Un esempio di crescita di questo tipo è quello dello sviluppo di un essere vivente dalla cellula che si è formata per l'unione di cellula uovo e spermatozoo: dopo un po' la cellula si scinde dando origine a due cellule, che a loro volta si scinderanno formando quattro cellule, e così via, quindi la successione che dà il numero di cellule dopo ogni scissione è: 1, 2, 4, 8, 16, ... , $2^n$,... ; naturalmente in realtà il processo è esattamente di questo tipo solo fino ad un certo punto, poi le cellule iniziano a differenziarsi formando le varie parti dell'organismo, e il loro modo di riprodursi si differenzia corrispondentemente.

Probabilmente l'espressione *crescita esponenziale* per indicare una forte crescita vi è familiare, ma un' occhiata più da vicino ai dati di un esempio può servire per avere un' idea più effettiva di cosa voglia dire *crescita esponenziale*.

Consideriamo la progressione geometrica: 3, 9, 27, 81, 243, ... , $3^n$,... data dalle potenze del tre (qui si ha $S(1) = 3^1 = 3$ , $S(n+1) = 3.S(n)$ ; oppure $S(n) = 3^n$ ). Pensiamo di rappresentare i suoi elementi con delle striscioline di carta ognuna dell'altezza, in cm, dell'elemento corrispondente; la prima sarà di 3cm, la seconda di 9cm, ... , la quinta misurerà $3^5 = 243$cm , alta come un armadio medio, la nona $3^9 = 19.683$cm, cioè alta come un grattacielo di una cinquantina di piani, la dodicesima $3^{12} = 531.441$cm, ben più alta del Monte Bianco, la diciannovesima $3^{19} = 1.162.261.467$cm , all'incirca la distanza della Luna dalla Terra !

Naturalmente le progressioni (aritmetiche o geometriche) non sono le sole successioni significative: consideriamo ad esempio questa: 1, 1, 2, 3, 5, 8, 13, 21, 34, ... Avete capito come prosegue? In questa successione, ogni elemento (a parte i primi due) è la somma dei due che lo precedono; per darla per ricorrenza bisogna assegnare i primi due elementi e poi la legge che abbiamo appena enunciato, così:

$$S(1) = 1\ ,\ S(2) = 1\ ,\ \ S(n+2) = S(n) + S(n+1)\ .$$

I numeri che compongono questa successione sono detti *numeri di Fibonacci,* dal nome del matematico pisano L. Fibonacci (circa 1170-1240) il quale li introdusse come soluzioni del seguente problema. Supponiamo che una coppia di conigli diventa capace di riprodursi dopo un anno dalla nascita, e che poi produca un'altra coppia di conigli ogni anno. Se parto con una coppia appena nata, quante coppie di conigli avrò ogni anno?

La situazione è riassunta nella tabella seguente:

| **A: Coppie conigli Giovani** | **B: Coppie conigli adulti** | **C: Coppie conigli in totale** |
|---|---|---|
| **1** | **-** | **1** |
| **-** | **1** | **1** |
| **1** | **1** | **2** |
| **1** | **2** | **3** |
| **2** | **3** | **5** |
| **3** | **5** | **8** |
| **5** | **8** | **13** |
| **8** | **13** | **21** |
| . . . | . . . | . . . |

Come si può vedere, si parte il primo anno con una sola coppia giovane; il secondo anno avremo ancora una coppia, però adulta, quindi al terzo anno essa avrà generato una nuova coppia giovane (in totale avremo 2 coppie), al quarto anno la coppia adulta ci ha dato una coppia giovane, mentre quella giovane che avevamo si è sviluppata, e ne abbiamo quindi 2 adulte (3 in totale).

Ad ogni anno la situazione sarà la seguente:

- in colonna **B** avrò quello che all'anno prima avevo in colonna **C** , in quanto tutte le coppie che avevo il precedente anno ora sono adulte,
- in colonna **A** avrò il numero che avevo l'anno prima in colonna **B**, in quanto tutte le coppie adulte hanno figliato.

La quantità in **A** sarà anche uguale a quello che avevo due anni prima in colonna **C**, per quanto abbiamo appena detto su come è fatta la colonna **B**, quindi in totale (in **C**) avrò la somma dei totali dei due anni precedenti (sempre le quantità in **C**) .