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 $\{2, 3, 5, ..., p_n\}$. 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 ($a \mod p_k = 1$, quindi p_k non divide p) ed è più grande di p_k che quindi non è il primo più grande di tutti. 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?