Giulio Cesare Barozzi

CONVERGENZE

Aritmetica:
un approccio computazionale

Springer

UMI - CIIM

Convergenze

a cura di
F. Arzarello, L. Giacardi, B. Lazzari

Giulio Cesare Barozzi

Aritmetica:
un approccio computazionale

Springer

Giulio Cesare Barozzi
Università degli Studi di Bologna

ISBN 978-88-470-0581-5

Springer fa parte di Springer Science+Business Media
springer.com

Stampato in Italia

Riprodotto da copia camera-ready fornita dall'autore
Progetto grafico della copertina: Valentina Greco, Milano
Stampa: Arti Grafiche Nidasio, Milano

Prefazione

Questo testo trae spunto dalle note di un corso di aggiornamento rivolto ad un gruppo di docenti delle scuole superiori. Con l'occasione esso è stato riveduto, corretto e ampliato, e sono state introdotte indicazioni per l'uso dei più diffusi sistemi di calcolo algebrico: Derive, Maple e Mathematica.

Il volumetto che ne è risultato vuole essere un invito allo studio della teoria dei numeri, in vista del quale, al termine, vengono date opportune indicazioni bibliografiche.

Desidero ringraziare Sebastiano Cappuccio, Ercole Castagnola, Michele Impedovo ed Enrico Pontorno che hanno letto una prima stesura del testo, segnalando errori e suggerendo miglioramenti.

All'Unione Matematica Italiana va il mio ringraziamento per aver voluto inserire questo volumetto nella collana Convergenze; sono debitore ai due anonimi recensori di alcuni suggerimenti e segnalazioni che ho cercato di accogliere nei limiti che mi ero imposto.

Bologna, settembre 2006

Giulio Cesare Barozzi
gcbarozzi@mac.com

Indice

1
Numeri interi

La sabbia del mare, le gocce della pioggia
e i giorni del mondo chi potrà contarli?
– Siracide **1**, 2

L'ambiente in cui ci muoveremo nei primi tre capitoli di questo testo è l'insieme $\mathbb{Z}$ dei numeri interi. Ricordiamo che $\mathbb{Z}$ è costituito dall'insieme $\mathbb{N}$ dei numeri naturali (zero incluso) e dai loro opposti. In molti testi $\mathbb{Z}$ viene costruito come ampliamento di $\mathbb{N}$ e quest'ultimo può essere individuato mediante i cosiddetti *assiomi di Peano*, dal nome del matematico Giuseppe Peano (1858-1932) che li propose nel 1889 nel volume *Arithmetices principia*.

Ecco una possibile formulazione di tali assiomi: $\mathbb{N}$ è un insieme contenente un elemento indicato con il simbolo 0 (zero), ed esiste un'applicazione iniettiva σ da $\mathbb{N}$ a $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$, tale che se A è un sottoinsieme di $\mathbb{N}$ per cui sono verificate le proprietà

i) $0 \in A$

ii) $x \in A$ implica $\sigma(x) \in A$

allora necessariamente $A = \mathbb{N}$.

L'elemento $\sigma(x)$ si chiama *successivo* di x. L'iniettività di σ significa che numeri naturali distinti ammettono sucessivi distinti; l'unico sottoinsieme di $\mathbb{N}$ che goda delle proprietà di contenere 0 e di contenere il successivo di ogni suo elemento è $\mathbb{N}$ stesso.

Si osservi che dall'iniettività di σ segue la suriettività: infatti l'insieme $A := \{0\} \cup \sigma(\mathbb{N})$ gode delle proprietà i) e ii). Se ne conclude che ogni numero naturale diverso da 0 è il successivo di un ben definito numero naturale.

A partire dalla nozione di successivo si può definire l'addizione in $\mathbb{N}$: se $n = 0$, si pone

$$n + m := m;$$

in caso contrario, cioè se $n \in \mathbb{N}^*$, dunque $n = \sigma(n')$ per un opportuno $n' \in \mathbb{N}$, si pone

$$n + m = \sigma(n') + m := \sigma(n' + m).$$

Si verificano senza difficoltà le proprietà commutativa e associativa dell'addizione.

La moltiplicazione tra numeri naturali può essere definita a partire dall'addizione. Se $n = 0$ si pone

$nm := 0$;

altrimenti si pone

$$nm = \sigma(n')\, m := n'm + m.$$

Le definizioni poste sono di tipo ricorsivo. Ad esempio, poiché $1 = \sigma(0)$, si ha $1 \cdot m = 0 \cdot m + m = m$; poiché $2 = \sigma(1)$, si ha $2 \cdot m = 1 \cdot m + m = m + m$, e così via.

Si verificano le proprietà commutativa e associativa della moltiplicazione nonché la proprietà distributiva della moltiplicazione rispetto all'addizione.

Le operazioni di addizione e moltiplicazione sono "leggi di composizione interna" ad $\mathbb{N}$; gli elementi neutri sono rispettivamente 0 e 1. Infine si ha (sempre in $\mathbb{N}$)

$$n + m = 0 \quad \Longleftrightarrow \quad n = m = 0.$$

La definizione della moltiplicazione tra numeri naturali, ricondotta all'addizione, si traduce direttamente in un qualunque linguaggio di programmazione che ammetta la ricorsione.

Ecco una versione scritta nel linguaggio TI-BASIC (il linguaggio delle calcolatrici grafico-simboliche della Texas Instruments):

```
:mult(n,m)
:Func
:When(n = 0, 0, mult(n-1, m) + m)
:EndFunc
```

Possiamo anche fornire una versione iterativa dell'algoritmo di moltiplicazione: il prodotto nm viene calcolato come somma di n "repliche" dell'addendo m.

ALGORITMO 1.1 - Moltiplicazione tra numeri naturali (1° versione).

Dati i numeri $n, m \in \mathbb{N}$, si calcola $p := nm$.

0. $n \to N,\ m \to M$
1. $0 \to P$
2. finché $N > 0$, ripetere:
2.1 $\quad P + M \to P$
2.2 $\quad N - 1 \to N$
3. stampare P
4. fine.

Nella precedente descrizione abbiamo fatto uso di tre variabili, N, M e P, ciascuna in grado di assumere valori naturali; nella traduzione in un programma per un calcolatore possiamo supporre che tali variabili siano associate ad altrettanti *registri* (o *celle*) della memoria: ad ogni variabile può

essere assegnato un solo valore alla volta, il contenuto attuale del corrispondente registro. Prescinderemo, per ora, da limitazioni inerenti la capacità dei registri.

L'operazione di *assegnazione* di un valore ad una variabile è indicata col simbolo $\rightarrow$; tale simbolo ha dunque lo stesso significato del simbolo := del linguaggio Pascal.

Nell'istruzione 0 alle variabili N e M si assegnano i valori n e m rispettivamente; si tratta della cosiddetta *inizializzazione* delle variabili in questione (in un programma che traduca l'algoritmo, si tratta dall'acquisizione dei dati in ingresso dall'esterno del programma stesso).

Nelle istruzioni 2.1 e 2.2 le variabili N e P compaiono tanto a sinistra quanto a destra del simbolo di assegnazione. L'interpretazione è questa: si valuta innanzitutto l'espressione che sta scritta a sinistra del simbolo di assegnazione, ed il valore ottenuto viene assegnato alla variabile che sta scritta a destra, cancellando automaticamente il valore precedentemente attribuito ad essa.

Dunque, ogni volta che viene eseguita l'istruzione 2.1 il contenuto di P viene aumentato della quantità m, assegnata alla variabile M, mentre l'istruzione 2.2 provvede a diminuire di un'unità il valore assegnato ad N.

Si osservi che, dopo ogni esecuzione delle due istruzioni contenute al passo 2, la quantità $NM + P$ si mantiene *invariante*: essa ha il valore nm, lo stesso posseduto dopo che le tre variabili in gioco sono state inizializzate. La variabile N svolge il ruolo di *contatore*: essa conta quante volte viene eseguito il blocco di istruzioni contenute al passo 2.

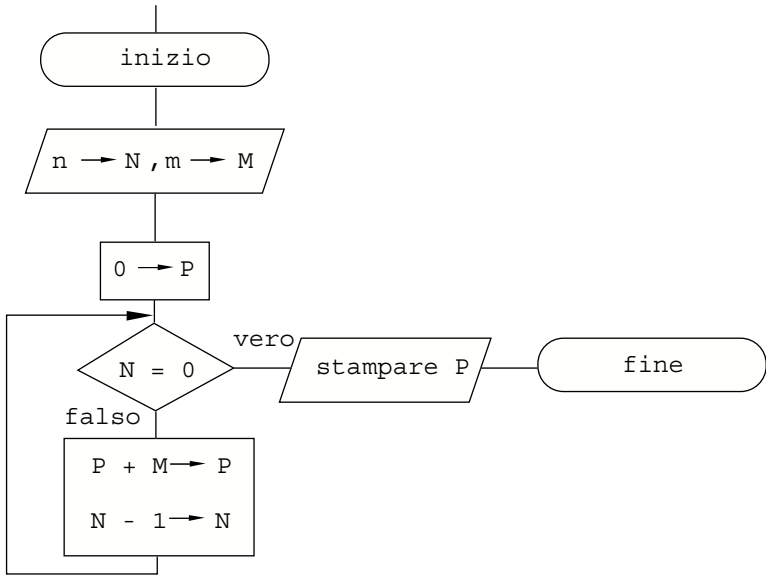

Figura 1.1 Diagramma di flusso dell'algoritmo 1.1.

L'istruzione 3 significa che, al termine dell'algoritmo, il valore finale del registro P viene reso disponibile all'esterno; naturalmente, la frase "stampare P" non va presa alla lettera: se si dispone soltanto di una calcolatrice munita di un visore, si farà in modo che il valore finale di P compaia su di esso per essere letto ed eventualmente trascritto.

L'algoritmo 1.1 può essere descritto, in forma equivalente, mediante il diagramma di flusso (in inglese: *flow-chart*) mostrato nella figura 1.1. Le operazioni di ingresso e uscita sono descritte entro parallelogrammi, le operazioni vere e proprie entro rettangoli, i confronti entro rombi: l'algoritmo procede in modi diversi secondo l'esito del confronto eseguito.

La traduzione dell'algoritmo 1.1 nel linguaggio TI-BASIC (o altri linguaggi simili) è immediata:

```
:multit(n,m)
:Func
:Local p
:0 → p
:While n > 0
:p+m → p :n-1 → n
:EndWhile
:Return p
:EndFunc
```

La terza istruzione significa che la variabile `p` è *locale*, cioè viene utilizzata soltanto all'interno della funzione che abbiamo chiamato `multit`. La penultima istruzione significa che il valore finale di `p` viene mostrato sul visore della calcolatrice.

Vogliamo ora definire l'insieme $\mathbb{Z}$ degli interi come un ampliamento di $\mathbb{N}$ in cui sia possibile simmetrizzare l'addizione. Un modello dell'insieme degli interi può essere costruito nel modo seguente. Consideriamo l'insieme delle coppie ordinate di numeri naturali (sottoinsieme di $\mathbb{N} \times \mathbb{N}$) aventi almeno un elemento nullo, cioè l'insieme delle coppie del tipo $(n, 0)$ oppure $(0, m)$, con $n, m \in \mathbb{N}$.

Definiamo l'addizione in tale insieme in modo tale che, a costruzione avvenuta, il sottoinsieme costituito dalle coppie $(n, 0)$ abbia la stessa struttura (cioè sia "isomorfo") ad $\mathbb{N}$. Poniamo

$$(n,0) + (m,0) := (n+m,0), \quad (0,n) + (0,m) := (0,n+m)$$

$$(n,0) + (0,m) := \begin{cases} (n-m,0), & \text{se } n \geq m, \\ (0,m-n), & \text{altrimenti.} \end{cases}$$

La scrittura $n \geq m$ significa che esiste $d \in \mathbb{N}$ tale che $m + d = n$. Tale numero d viene indicato $n - m$. Se poi $n \geq m$ e $n \neq m$, scriveremo $n > m$.

Non è difficile verificare che l'addizione così definita è commutativa e associativa; l'elemento neutro è $(0, 0)$, mentre gli elementi $(n, 0)$ e $(0, n)$ sono opposti tra loro.

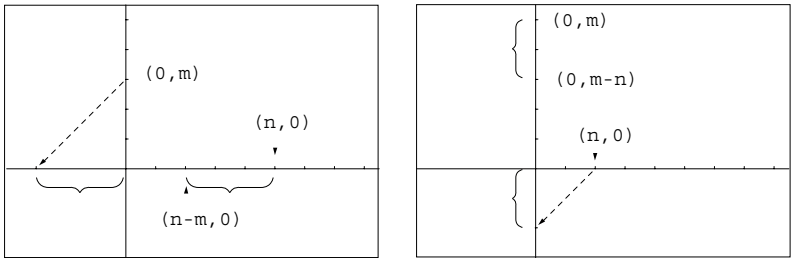

Figura 1.2 La somma di $(n,0)$ e $(0,m)$ è $(n-m,0)$ se $n \geq m$, è $(0,m-n)$ se $n < m$.

la moltiplicazione viene definita ponendo

$$(n,0)\cdot(m,0) = (0,n)\cdot(0,m) := (nm,0),$$

$$(n,0)\cdot(0,m) = (0,n)\cdot(m,0) := (0,nm).$$

Si verificano per la moltiplicazione le proprietà associativa e commutativa; (1,0) è l'elemento neutro della moltiplicazione e quest'ultima è distributiva rispetto all'addizione.

L'insieme delle coppie del tipo $(n,0)$, essendo isomorfo ad $\mathbb{N}$ tramite l'isomorfismo

$$(n,0) \mapsto n,$$

verrà semplicemente identificato con $\mathbb{N}$; in questo senso si può dire che $\mathbb{N}$ è contenuto in $\mathbb{Z}$, nonché scrivere n al posto di $(n,0)$ e $-n$ al posto di $(0,n)$. Porremo ancora

$$n - m := n + (-m).$$

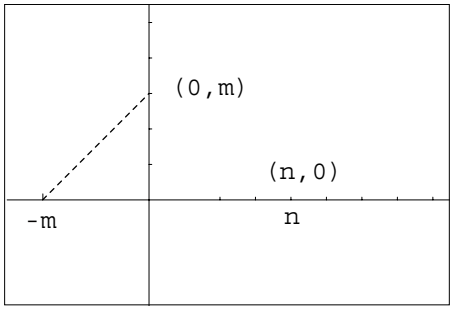

Figura 1.3 L'intero $(n,0)$ viene identificato con n, l'intero $(0,m)$ con $-m$.

L'insieme $\mathbb{Z}$ (munito delle operazioni di addizione e moltiplicazione) possiede una struttura di anello commutativo (con unità); tale struttura è sintetizzata dalla Tabella 1.1. Si osservi che, per ogni $n \in \mathbb{Z}$, si ha una delle alternative

$$n = 0, \quad n \in \mathbb{N}^*, \quad -n \in \mathbb{N}^* \quad \text{(legge di tricotomia)}.$$

Osserviamo ancora che $\mathbb{Z}$ è un *dominio di integrità*, cioè vale la *legge di annullamento del prodotto*:

$$(nm = 0) \quad \Longrightarrow \quad (n = 0 \ \vee \ m = 0),$$

o, in forma equivalente

$$(n \neq 0 \ \wedge \ m \neq 0) \quad \Longrightarrow \quad (nm \neq 0).$$

Possiamo infine definire una relazione di *ordine totale* in $\mathbb{Z}$ ponendo

$$n \leq m \quad \Longleftrightarrow \quad m - n \in \mathbb{N};$$

la scrittura $n < m$ significa $n \leq m$ e $n \neq m$, cioè $m - n \in \mathbb{N}^*$. La relazione così introdotta in $\mathbb{Z}$ è compatibile con le operazioni, nel senso che, per ogni $n, m, p \in \mathbb{Z}$, si ha

$$n \leq m \quad \Longrightarrow \quad n + p \leq m + p,$$

e, per ogni $n, m \in \mathbb{Z}$ e per ogni $p \in \mathbb{N}$, si ha

$$n \leq m \quad \Longrightarrow \quad np \leq mp.$$

Tabella 1.1 Struttura dell'anello $\mathbb{Z}$ degli interi.

$(x + y) + z = x + (y + z), \quad (xy)z = x(yz)$ (proprietà associativa)
$x + y = y + x, \quad xy = yx$ (proprietà commutativa)
Esiste un elemento, denotato 0 (zero), tale che $x + 0 = x$ per ogni x (esistenza del neutro additivo)
Esiste un elemento $\neq 0$, denotato 1 (uno) tale che $1 \cdot x = x$ per ogni x (esistenza del neutro moltiplicativo)
$x(y + z) = xy + xz$ (proprietà distributiva)
Per ogni x esiste y tale che $x + y = 0$ (esistenza del simmetrico additivo (= opposto))

Occupiamoci ora della divisione tra numeri interi; cominciamo dal caso dei numeri naturali: dati $n \in \mathbb{N}$ e $m \in \mathbb{N}^*$, se esiste $q \in \mathbb{N}$ tale che

$$n = qm$$

diremo che m è un *divisore* di m (oppure che n è un *multiplo* di m) e l'intero q viene chiamato *quoziente* della divisione di n per m. La divisibilità di n per

m è una circostanza in un certo senso eccezionale; se n non è divisibile per m, possiamo eseguire la "divisione con resto", cioè possiamo cercare due numeri naturali q ed r tali che sia

$$n = qm + r \tag{1}$$

con la condizione ulteriore che si abbia

$$0 \leq r < m. \tag{2}$$

Non è difficile verificare che l'ultima condizione imposta individua univocamente q ed r (si veda l'esercizio 1.1 al termine del capitolo); il procedimento che vedremo tra un istante ci consentirà di dimostrare costruttivamente l'esistenza dei due numeri cercati. Tale procedimento è spesso citato come *divisione euclidea*, in quanto esso riproduce sostanzialmente quello descritto da Euclide, utilizzando un linguaggio geometrico, nel Libro VII (Prop. 1 e 2) degli *Elementi*. Lo scopo di Euclide è il calcolo del massimo comune divisore tra due interi positivi, e la divisione con resto, più precisamente la determinazione del solo resto, viene utilizzata come passo intermedio per ottenere tale scopo.

L'idea di Euclide è semplice. Innanzitutto, se $0 \leq n < m$, allora $q = 0$ e $r = n$. In caso contrario, cioè se $0 < m \leq n$, si sottrae m da n tante volte quant'è necessario perché il *resto*, cioè la quantità che rimane, scenda al disotto di m. Il quoziente q si ottiene contando quante volte m è stato sottratto da n per arrivare ad un resto inferiore ad m.

Ad esempio, se $n = 14$ e $m = 4$, poiché $n > m$, eseguiamo ripetutamente la sottrazione della costante 4 a partire da 14, ottenendo in sequenza i valori 10, 6, 2; dopo 3 sottrazioni abbiamo ottenuto il valore 2 minore di 4, quindi $q = 3$, $r = 2$. Infatti

$$14 = 3 \cdot 4 + 2.$$

ALGORITMO 1.2 - Divisione euclidea (prima versione).

Dati i numeri $n \in \mathbb{N}$ e $m \in \mathbb{N}^*$, si calcolano $q, r \in \mathbb{N}$ tali che $n = qm + r$, con $0 \leq r < m$.

0. $n \to R$, $m \to M$
1. $0 \to Q$
2. finché $R \geq M$, ripetere:
2.1 $\quad Q + 1 \to Q$
2.2 $\quad R - M \to R$
3. stampare Q, R
4. fine.

Si osservi che, dopo ogni esecuzione del blocco di istruzioni contenute al passo 2, la quantità $QM + R$ si mantiene *invariante*: essa conserva il valore n assunto all'atto dell'inizializzazione delle variabili in gioco.