1

Capitolo B10
notazioni posizionali per gli interi

Contenuti delle sezioni

a. notazioni posizionali per i numeri naturali p. 2
b. sommatoria e produttoria p. 9
c. somma di naturali mediante notazioni posizionali p. 14
d. prodotto e quoziente di naturali mediante notazioni posizionali p. 18
e. produttoria cartesiana di insiemi finiti p. 23

24 pagine

B10 0.01 Questo capitolo è dedicato all'introduzione delle notazioni posizionali per i numeri interi cominciando da quelle per i numeri naturali.

Le notazioni posizionali saranno definite anche per i più generali numeri razionali, reali e complessi, anche se in gran parte in grado di fornire solo valori approssimati.

Si tratta di notazioni di grande importanza pratica in quanto consentono di controllare efficacemente buona gran parte delle entità formali utilizzate per esprimere considerazioni quantitative [P01c, P02a].

Infatti sulle notazioni posizionali possono essere definiti algoritmi e procedure in grado di governare efficientemente l'esecuzione effettiva di varie costruzioni numeriche a cominciare dalla esecuzione delle quattro operazioni aritmetiche: somma, differenza, prodotto e divisione.

Vedremo che le notazioni posizionali consentono di esprimmere numeri molto grandi con scritture relativamente contenute, in particolare notazioni degli interi naturali sostanzialmente più contenute delle notazioni unadiche.

Con le notazioni posizionali può essere maneggiata con una certa facilità, sia da parte degli esecutori umani che da parte degli artificiali, la massima parte dei numeri che servono per affrontare i problemi trattabili con metodi quantitativi.

Conviene tuttavia anticipare che taluni studi richiedono di manipolare numeri ancora più elevati di quelli che si presentano in campi come l'astrofisica, le particelle elementari e talune problematiche probabilistiche. Per questi numeri si devono adottare notazioni particolari, più complesse di quelle qui introdotte.

B10 a. notazioni posizionali per i numeri naturali

B10 a.01 Ci proponiamo ora di individuare notazioni che consentano di presentare in modo leggibile gli interi naturali e che forniscano scritture mediante le quali si possano eseguire efficientemente molti calcoli, a cominciare dalle somme e dai prodotti.

Abbiamo già visto che l'operazione di prodotto consente di esprimere alcuni interi naturali molto elevati mediante interi naturali di valore sensibilmente inferiore.

Ancora più vantaggiosa dal punto di vista della concisione può risultare l'operazione di elevamento a potenza, auspicabile generalizzazione del prodotto di un numero per se stesso.

Servendoci delle notazioni unadiche si avrebbe:

$$|||^{|||} = ||| \cdot ||| \cdot ||| = |||||||||||||||||||||||||$$

$$|||^{||||} = ||| \cdot ||| \cdot ||| \cdot ||| = ||||||||| \cdot ||||||||| =$$

$$|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||$$

Accade tuttavia che vi sono interi naturali che non si possono esprimere mediante prodotti e potenze di naturali di grandezze ragionevolmente ridotte. Questo si riscontra in particolare per i numeri primi [B20g] non piccoli, ad esempio per 113 e a maggior ragione per numeri esprimibili come $2^{82\,589\,933} - 1$. È invece cruciale individuare notazioni che permettano di trattare con efficacia tutti i naturali e che inoltre possano estendersi senza strappi ad altre entità numeriche.

B10 a.02 Un intero naturale m si dice **multiplo** di un intero positivo h sse si trova un intero naturale k tale che $m = h \cdot k$; in tal caso si dice che h **divide** m, o equivalentemente che h è **divisore** di m.

Di solito questa situazione si esprime concisamente scrivendo $h|m$. Qui preferiamo scrivere $h \preceq_: m$, scrittura nella quale il segno $\preceq_:$ sta a denotare un connettivo relazionale che [B18a04] si trova essere facilmente decidibile; il simbolo $\preceq_:$ qui preferito evidenzia la dissimmetria tra i due naturali che esso pone in collegamento.

L'intero positivo k dell'enunciato $m = h \cdot k$ si dice **quoto** o quoziente esatto tra m ed h e lo scriviamo $m : h := k$.

Con questa ultima scrittura si individua una operazione binaria parziale costruibile che a un naturale m e a un intero positivo h associa un altro naturale, ma solo per determinate scelte degli operandi m ed h.
Per esempio si constata che il quoto di 6 e 3 è 2, mentre non esiste alcun naturale che sia quoto tra 7 e 3.

Si osserva anche che ogni intero m è multiplo di 1 e che 0 si può considerare multiplo di ogni intero positivo h: queste affermazioni sono equivalenti, risp., agli enunciati $m : 1 = m$ e $0 : h = 0$.

Se $m = h \cdot k$ con k maggiore di 1 m si dice **multiplo proprio** di h e h si dice **divisore proprio** di m.

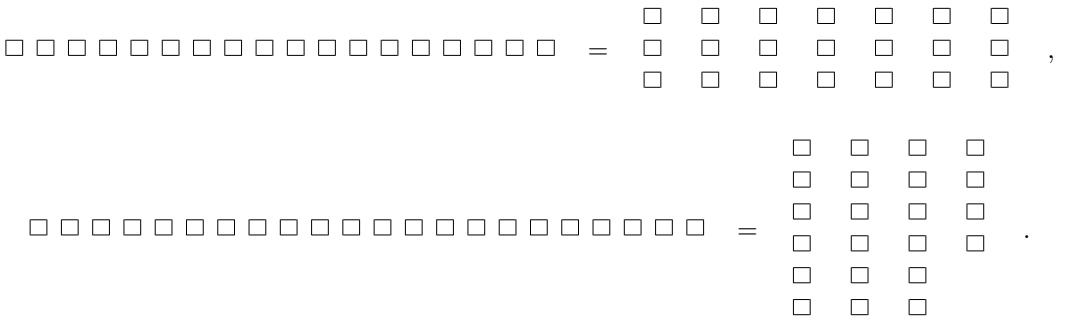
B10 a.03 Vogliamo ora utilizzare la notazione unadica per esaminare la divisibilità tra due interi positivi m ed h, ovvero per decidere se $h \preceq_: m$ o meno. Per questo conviene usare notazioni unadiche che non si servono del segno $|$, ma del segno $\square$.

Utilizzeremo due nastri modificabili T_m e T_h per i dati $\mathsf{notp}_1(m)$ e $\mathsf{notp}_1(h)$, risp., di un nastro di lavoro bidimensionale T_b e di un nastro di uscita T_q.

Con una iterazione primaria si procede a riprodurre (con una iterazione secondaria) sequenze di h segni $\square$ che si possono sottrarre dal nastro T_m e servendoci di T_q (come contatore) registriamo il numero delle riproduzioni che si possono effettuare; l'iterazione primaria prosegue fino a che su T_m rimangono meno di h segni $\square$ e in particolare quando T_m risulta svuotata dai segni $\square$. Si tratta quindi di una iterazione che si conclude con la constatazione della impossibilità di effettuare un ulteriore stadio.

Se su T_m non è rimasto alcun $\square$ si conclude che h divide m e che il numero di colonne complete su T_b registrato su T_q fornisce la rappresentazione unadica del quoto $m : h$.
In caso contrario, cioè se si finisce con un certo numero di righe sovrapposte su T_q e con un certo numero positivo r di $\square$ su T_m, si conclude che m non è multiplo di h.
Questa situazione si denota scrivendo $h \not\preceq_: m$, utilizzando il connettivo relazionale evidentemente decidibile $\not\preceq_:$ negazione di $\preceq_:$.

Sono riportati, qui di seguito, due esempi: se $m = 18$ ed $h = 3$ si conclude che 3 divide 18 e che $18 : 3 = 6$; se invece $m = 22$ ed $h = 6$ si arriva a concludere che 6 non divide 20.



B10 a.04 In un caso come il secondo riportato, l'intero positivo minore di h fornito dalla configurazione finale di T_m come raffigurazione della colonna incompleta si dice **resto** della divisione di 32 per 5; il resto della divisione di m per h, in accordo con molti linguaggi di programmazione, lo denoteremo con $m \,\%\, h$; esso è un intero compreso tra 0 e $m - 1$.

Evidentemente l'intero $m - m \,\%\, h$ è multiplo di h e viene detto **parte intera della divisione** di m per h; esso talora si denota con $m : h$, ma in seguito, per avere enunciati estendibili a numeri non interi, preferiamo denotarlo con $\left\lfloor \frac{m}{h} \right\rfloor$ o, equivalentemente, con $\lfloor m/h \rfloor$.

In generale quindi per ogni intero naturale m e ogni intero positivo h si ha:

$$m \;=\; \left\lfloor \frac{m}{h} \right\rfloor + m \,\%\, h \;.$$

Servendosi del resto $r := m \,\%\, h$, si scrive anche $m \equiv r \pmod{h}$, scrittura che si legge "m è congruo ad r modulo h".

Scriveremo anche $m \;=_h\; r$, denotando con $=_h$ un connettivo relazionale decidibile tra interi naturali che chiamiamo **congruenza modulo** h. Per tale connettivo, che tratteremo ampiamente in B26, quindi si ha $m =_h m \,\%\, h$. Si constata che questo connettivo esprime una relazione di equivalenza.

B10 a.05 Le operazioni e i connettivi precedenti si possono convenientemente estendere da $\mathbb{N}$ all'intero insieme dei numeri interi $\mathbb{Z}$.

Denotiamo con z è un intero qualsiasi da considerare variabile e ancora con h denotiamo un intero maggiore di 1.

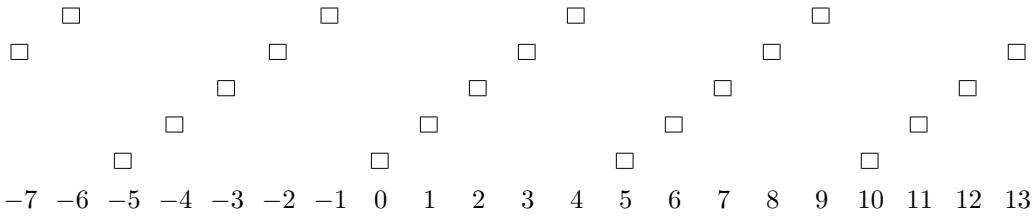
Estendiamo l'operazione unaria $z \,\%\, h$ chiedendo che mantenga la proprietà di invarianza nel caso di variazione di z per somma di un multiplo intero di h, cioè chiediamo che sia

$$\forall j \in \mathbb{Z} \;:\; (z + h \cdot j) \,\%\, h \;=\; z \,\%\, h \;.$$

Questa richiesta implica per esempio la seguente lista di coppie di valori $\langle z, z\%h \rangle$ per $h = 5$ e $z = -7, -6, ..., 12, 13$:

$$\left\downarrow \begin{array}{cccccccccccccccccccc} \text{-7} & \text{-6} & \text{-5} & \text{-4} & \text{-3} & \text{-2} & \text{-1} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 \end{array} \right\downarrow \;.$$

Questa lista viene opportunamente visualizzata dal seguente grafico



Dalle precedenti estensioni dell'operazione $\%$ e del connettivo $=_h$ seguono le seguenti proprietà valide per z e ζ interi qualsiasi e per h intero positivo qualsiasi:

$$z \;=\; \left\lfloor \frac{z}{h} \right\rfloor \cdot h + z \,\%\, h \;.$$

$$m \;=_h\; \zeta \quad \Longleftrightarrow \quad m \,\%\, h \;=\; \zeta \,\%\, h \;.$$

In particolare:

$$-19 \;=\; \left\lfloor \frac{-19}{7} \right\rfloor \cdot 7 + (-19) \,\%\, 7 = -3 \cdot 7 + 2 \;.$$

B10 a.06 Un numero intero si dice pari sse è multiplo di 2,cioè sse si può porre nella forma $2\,h$ per qualche h intero. I numeri naturali che non sono pari si dicono invece **dispari**; ciascuno di essi si può esprimere nella forma $2h + 1$ per qualche h intero.
Chiaramente un numero intero n è pari sse $n\%2 = 0$ ed è dispari sse $n\%2 = 1$.

Un qualsiasi numero intero n si può quindi porre nella forma $n = 2h_1 + b_0$ con h_1 intero e $b_0 \in \{0, 1\}$, ovvero $b_0 = 0, 1$.

Questa scrittura per n elevato porta a una notazione unadica un po' più concisa di quella per n; ma h_1 può ancora essere molto grande e quindi poco maneggevole.

Possiamo però applicare lo stesso meccanismo anche ad h_1 giungendo alla scrittura $h_1 = 2\,h_2 + b_1$ e quindi ottenendo $n = h_2\,2^2 + b_1\,2 + b_0$ con h_2 naturale e con $b_0, b_1 = 0, 1$.

Questa manovra di decomposizione del coefficiente della potenza più elevata di 2 può essere portata avanti fino a quando si ottiene una espressione

$$n \;=\; h_r\,2^r + b_{r-1}\,2^{r-1} + \cdots + b_1\,2 + b_0 \;,$$

con il primo coefficiente uguale ad 1, cioè con $h_r = b_r = 1$.

A questo punto non ha senso proseguire, in quanto è sicuro che si avrebbero nuovi addendi costituiti da ulteriori potenze di 2 moltiplicate per 0.
Questi addendi nulli in genere sono inutili; vedremo tuttavia che per alcune manovre conviene aggiungerli in un certo numero al fine di rendere più semplice la descrizione della manovra stessa.

Con il procedimento descritto si ottiene per esempio

$$||||||||||| \;=\; ||||| + 1\cdot 2^0 \;=\; ||\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 \;=\; 1\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0\ .$$

In generale, osservando che $2 = 2^1$ e che $1 = 2^0$, si ha che per ogni naturale n si può scrivere

$$n \;=\; b_r\cdot 2^r + b_{r-1}2^{r-1} + \cdots + b_1 2^1 + b_0 2^0\ ,$$

dove si conviene che sia $b_r = 1$, ma con la esclusione del caso $n = 0$ per il quale $r = 0$ e $b_0 = 0$.

Osserviamo che per individuare n basta la stringa di cifre binarie $b_h\, b_{h-1}\, ...\, b_1\, b_0$; questa stringa costituisce la cosiddetta **notazione binaria** o **codifica in base 2** del numero naturale n.

L'intero naturale r si dice **parte intera del logaritmo in base 2 di** n [v.a. a09].

B10 a.07 La espressione che ha portato alla codifica binaria di un naturale può interpretarsi visivamente come suddivisione dell'insieme dei segni che costituiscono la codifica unadica di n in un certo numero di sottoinsiemi con cardinali dati da diverse potenze di 2. Più precisamente per la potenza i-esima è presente il sottoinsieme che rappresenta 2^i sse $b_i = 1$.

Per esempio si hanno le seguenti riorganizzazioni di segni:

La scrittura 1101_2 introdotta sopra serve a rappresentare la sequenza binaria $b_3\, b_2\, b_1\, b_0$ con $b_3 = 1,\ b_2 = 1,\ b_1 = 0,\ b_0 = 1$ e si dice **notazione binaria** del dato numero (che impareremo a scrivere "13" e talora, quando dobbiamo essere completamente espliciti, "13_{10}") .

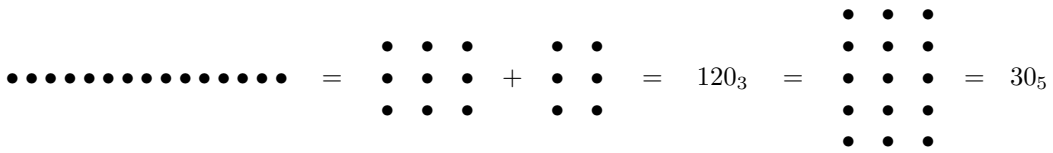
In generale la notazione binaria di un numero positivo è costituita da una sequenza binaria con il bit iniziale uguale a 1 e avente a deponente 2; per il numero naturale 0 si usa invece la scrittura binaria 0_2 che in genere si può abbreviare con la semplice cifra "0".

B10 a.08 Consideriamo un generico intero B maggiore di 1 e l'insieme $\mathbf{[}B\mathbf{)} = \{0, 1, ..., B-1\}$ dei primi B naturali. Associamo a ciascuno degli interi in questo insieme un segno peculiare che lo rappresenti; questi segni in numero di B li chiamiamo **cifre in base** B.
In precedenza abbiamo introdotto le cifre decimali 0, 1, 2, ..., 9; per operare in una base $B \le 10$ basta servirsi solo delle prime B cifre decimali.

Per servirsi di una base $B > 10$ occorre servirsi di altri segni: ad esempio per trattare varie informazioni per il computer spesso si opera nella base $|||||||||||||||| \;=\; 16_{10}$ servendosi delle cifre decimali e delle cifre $a = 10$, $b = 11$, $c = 12$, $d = 13$, $e = 14$, $f = 15$.

Con considerazioni del tutto simili alle precedenti relative a $B = 2$ si trova che un intero positivo n si può scrivere $n \;=\; h_1\cdot B + c_0$ e successivamente $n = h_2\cdot B^2 + c_1\cdot B + c_0$, ... , fino a giungere alla uguaglianza $n \;=\; c_h\cdot B^h + c_{h-1}\cdot B^{h-1} + ... + c_1 B + c_0$, dove per i coefficienti delle potenze B^i deve essere $c_i \in \{0, 1, \cdots, B-1\}$ e $c_h > 0$, fatta eccezione, come per $B = 2$, per il numero $n = 0$; per questo si può usare la scrittura 0_B o l'abbreviazione costituita dal semplice segno 0.

Per esempio con $B = 3$ e $B = 5$ per il numero comunemente usualmente scritto "15" abbiamo



B10 a.09 Si osserva che, assunto il numero naturale B maggiore o uguale a 2 come base, per individuare n è sufficiente la stringa $c_h\, c_{h-1} \ldots c_1\, c_0$ formata da h cifre in base B. Questa viene detta **notazione posizionale in base B di n** o **scrittura in base B di n**.
Più specificamente, come per $B = 2$ si è parlato di notazione binaria, per $B = 8$ si parla di scrittura o **notazione ottale**, per $B = 10$ di scrittura o **notazione decimale**, per $B = 16$ di scrittura o **notazione esadecimale**.

Quando si trattano scritture di numeri (naturali) in diverse basi, occorre aggiungere a ciascuna di esse come deponente la scrittura decimale della base adottata. Abbiamo quindi relazioni come le seguenti:

$$|||||||| = 8_{10} = 1000_2, \qquad 31_{10} = 37_8 = 11111_2, \qquad ab_{16} = 10101011_2 = 253_8 = 171_{10}\ .$$

Se $n > 0$ la lunghezza della scrittura in base B di n diminuita di 1 viene chiamata **parte intera del logaritmo in base B di n** o **logaritmo troncato in base B di n**; per tale intero positivo usiamo la notazione $\mathsf{Logtr}_B(n)$.

Per i valori del logaritmo troncato in base 2 abbiamo

$$\mathsf{Logtr}_2 = \begin{array}{cccccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \cdots & 15 & 16 & 17 & \cdots \\ 0 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & \cdots & 3 & 4 & 4 & \cdots \end{array}$$

Abbiamo inoltre $\mathsf{Logtr}_B(B) = 1$, $n < B \Longrightarrow \mathsf{Logtr}_B(n) = 0$, $\mathsf{Logtr}_4(5) = 1$, $\mathsf{Logtr}_4(15) = 1$, $\mathsf{Logtr}_4(16) = \mathsf{Logtr}_4(17) = 2$.

B10 a.10 Le scritture precedenti vengono chiamate collettivamente scritture posizionali o **notazioni posizionali** degli interi naturali.

La scrittura ottale di un naturale n da destra a sinistra si ottiene sostituendo ogni terna di cifre binarie incontrate con la corrispondente cifra in base 8; se il numero delle cifre binarie non è multiplo di 3, basta applicare il criterio precedente alla scrittura binaria completata con l'aggiunta di uno o due cifre 0 iniziali.

Si hanno quindi relazioni come $460_{10} = 111001100_2 = 714_8$, $157_{10} = 10011101_2 = 235_8$, $64 + 59 = 123_{10} = 1111011_2 = 001111011_2 = 173_8$.

Si svolgono considerazioni analoghe per le notazioni in base 4 e 16. La notazione in base 4 (la esadecimale) si ottiene dalla notazione binaria procedendo da destra a sinistra e sostituendo ogni coppia (ogni quaterna) di bits individuata con una cifra in base 4 (cifra esadecimale.
Per esempio si ha $175_{10} = 10101111_2 = cf_{16} = 2233_4$.

La notazione posizionale meno concisa è la binaria e passando da una base a una maggiore la lunghezza della notazione rimane invariata per alcuni numeri piccoli, mentre diminuisce per i numeri più grandi.

Le notazioni posizionali nelle diverse basi $B = 2, 3, \ldots$ presentano differenze di lunghezze che si possono giudicare contenute. Le lunghezze delle codifiche nelle diverse basi grosso modo differiscono per fattori moltiplicativi dati dai rapporti tra le corrispondenti parti intere dei logaritmi nelle rispettive basi.

Le notazioni posizionali consentono di esprimere agevolmente la massima parte dei numeri che rivestono interesse pratico e che non si devono considerare enormemente grandi; queste notazioni inoltre consentono di manipolare i numeri naturali (e non solo) con manovre non molto impegnative, senza sostanziali differenze quando si usano basi diverse.

La scrittura unadica di numeri elevati è invece sostanzialmente più lunga delle scritture posizionali nelle basi maggiori di 1.

In seguito potremo dire con maggiore precisione che la scrittura unadica con il crescere della sua lunghezza "aumenta esponenzialmente" rispetto alla corrispondente notazione in una qualsiasi base $B > 1$.

Si osserva che il significato delle prolisse scritture unadiche si spiega con poche parole, mentre le più concise notazioni posizionali sono portatrici di un significato la cui spiegazione, anche se oggi ampiamente ecomprensivbile, è sensibilmente più elaborata.

In effetti essa si è sviluppata nell'ambito della scienza indiana tra il I e il IV secolo d.C. (in particolare con Aryabhata di Kusumapura e Brahmagupta utilizzatore dello zero), è stata raccolta dai pensatori arabi e persiani (in particolare da Al-Kwaritmi e Omar kahyyam) che la chiamarono inizialmente "numerazione sulla polvere", solo successivamente è passata dal Maghreb alla Spagna (anno 976), si è diffusa nell'Europa occidentale anche grazie alla opera di Fibonacci), è stata adottata nella Cina intorno al 1300, in Russia Pietro il Grande all'inizio del XVIII secolo

Nelle notazioni posizionali si può vedere un compromesso tra lunghezza della definizione e lunghezza delle scritture da adottare.
Dei compromessi di questo genere si devono raggiungere per molti altri strumenti di calcolo, della matematica e delle scienze in genere.

B10 a.11 Intendiamo ora definire con precisione procedimenti che consentano di eseguire le operazioni sopra gli interi naturali manipolando sopra le loro notazioni posizionali. In queste considerazioni conviene distinguere un intero n dalla sua notazione posizionale in base B per la quale si adotta la scrittura $\mathsf{notp}_B(n)$.

Dato che le notazioni decimali sono quelle usate più frequentemente, le altre essendo usate solo in contesti particolari, di solito si semplificano le notazioni decimali sottintendendo il deponente $_{10}$ e utilizzando scritture specifiche come $\mathsf{notd}(n)$.

Cominciamo con l'operazione **passaggio all'intero successivo**, cioè con la trasformazione di un naturale n in $n+1$. Si tratta di una operazione semplice e fondamentale; in effetti, come vedremo, essa interviene nella impostazione assiomatica della teoria dei numeri interi [B65e].
Questa operazione sulle notazioni unadiche consiste nella ovvia aggiunta di un segno | alla stringa rappresentativa dell'intero precedente: $\mathsf{notp}_1(n+1) \;=\; \mathsf{notp}_1(n)\,|$.

In una base B per la rappresentazione del naturale n scriviamo

$$\mathsf{notp}_B(n) \;=:\; c_h\, c_{h-1} \ldots c_2\, c_1\, c_0 \ .$$

Paragonando due diverse occorrenze di cifre c_i e c_j, diciamo che c_i è la **cifra più pesante** di c_j sse si trova alla sua sinistra, ovvero sse $i > j$, ovvero sse c_i è il coefficiente della potenza B^i maggiore della B^j di cui è coefficiente c_j.

Per realizzare la trasformazione della stringa $Ntn_B(n)$ nella $Ntn_B(n+1)$ bisogna organizzare lo scorrimento della stringa data cominciando con la cifra più leggera c_0 e proseguendo con le cifre via via più pesanti, quelle che si trovano muovendosi verso sinistra.

Per ogni posizione j si cerca di trasformare c_j nella cifra nella successiva $c_j + 1$.
Se questo è possibile, cioè sse $c_j < B-1$, il procedimento è concluso; in caso contrario, cioè sse $c_j = B-1$, si trasforma questa cifra in 0 e si passa a effettuare il tentativo di aumentare la cifra immediatamente più pesante c_{j+1}.
Se si giunge a cercare di aumentare la cifra più pesante c_h e se questa non è aumentabile, cioè se $c_h = B-1$, la si trasforma in 0 e si aggiunge la cifra 1 come carattere iniziale di $Ntn(n+1)$, cioè come coefficiente di B^{h+1}. In tal caso si ottiene la notazione che inizia con 1 ed è seguita da $h+1$ repliche della

cifra 0 e dunque si aumenta di 1 la lunghezza della notazione, $\mathsf{len}(Ntn_B(n+1)) = \mathsf{len}(Ntn_B(n)) + 1$ (avendo quindi $\mathsf{Logtr}_B(n+1) = \mathsf{Logtr}_B(n) + 1$).

Gli effetti di questo algoritmo vengono esemplificati chiaramente da trasformazioni come le seguenti:

$125_{10} \longrightarrow 126_{10},\ \ 203_4 \longrightarrow 210_4,\ \ 2777_8 \longrightarrow 3000_8,\ \ 100111_2 \longrightarrow 101000_2,\ \ 222222_3 \longrightarrow 1000000_3$.

B10 a.12 Introduciamo ora una distinzione fondamentale entro i numeri naturali che non svilupperemo qui di seguito ma che conviene anticipare con una prima presentazione poco impegnativa.

Si dice **numero primo** ogni intero superiore ad 1 che si può dividere solo per se stesso e per 1.

Ricollegandoci al paragrafo a04 i numeri primi si possono descrivere come i numeri positivi che non si possono raffigurare con schieramenti rettangolari di segni □ con lati maggiori o uguali a 2.

In altre parole i numeri primi sono esattamente (cioè tutti e soli) i numeri interi maggiori di 1 che non si possono esprimere come prodotti di due numeri interi maggiori di 1.

I numeri primi più piccoli si trovano facilmente eliminando da un elenco di numeri maggiori di 1 quelli che risultano multipli di un intero precedente.

Con questa manovra si verifica facilmente che i numeri primi inferiori a 100 sono 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

I numeri primi risultano essenziali per affrontare molti problemi della matematica e per alcune sue applicazioni di grande rilevanza pratica, ad esempio per molti problemi dell'industria delle telecomunicazioni [v. in particolare `Crittografia (we)` e C66].

Per enunciare concisamente che un intero naturale p è un numero primo usiamo la notazione $p \in \mathsf{PRM}$, nella quale il simbolo PRM viene usato come notazione per l'insieme dei numeri primi.
Questa entità a questo punto si può considerare un insieme-B, in quanto è facilmente pensabile un procedimento per decidere se un numero naturale dato possegga o meno divisori propri, diversi da se stesso e da 1.

B10 b. sommatoria e produttoria

B10 b.01 Prima di chiarire come si possono effettuare le operazioni di somma e prodotto di interi positivi operando sulle notazioni posizionali è opportuno introdurre le notazioni di sommatoria e produttoria. Questi sono due costrutti contraddistinti da simboli peculiari che estendono le operazioni di somma e prodotto. Essi fanno parte di un insieme di simboli ciascuno dei quali ha un ruolo centrale in espressioni che coinvolgono intere sequenze di oggetti matematici che sono stati definiti in precedenza o si suppongono tali.
Di questo insieme di simboli fanno parte anche i segni che estendono gli operatori insiemistici binari esprimenti unione, intersezione, differenza simmetrica e prodotto cartesiano di insiemi visti in precedenza [B08e].
Per questi simboli derivati da operatori binari proponiamo il nome **operatori multiari**.

In questa sezione introduciamo solo i costrutti di sommatoria e produttoria da applicare ai numeri naturali e le accennate estensioni di unione e intersezione, limitandoci a composizioni di insiemi finiti di entità matematiche. Più oltre vedremo come questi costrutti si possano applicare a sequenze di molti altri tipi di numeri e di insiemi e come si possano definire vari costrutti applicabili a raggruppamenti non necessariamente finiti e di entità non necessariamente omogenee [T15, T16] .

B10 b.02 Molti problemi per essere risolti richiedono di trattare interi raggruppamenti di numeri, di insiemi o di altre entità sottoponibili a composizioni binarie o a trasformazioni.
Abbiamo già accennato alla opportunità di individuare le entità da comporre o trasformare espresse da simboli sia semplici che compositi muniti di indici (posti a deponente o a esponente dei simboli) il cui valore varia (corre) in una determinata sequenza di valori.

Cominciamo a considerare particolari somme di più numeri naturali espressi da simboli muniti di un solo indice.
Per esprimere tali composizioni si introducono scritture come le seguenti:

$$a_p + a_q + a_r =: \sum_{i\in\{p,q,r\}} a_i; \qquad b_1 + b_2 + b_3 + b_4 =: \sum_{i\in\{1,2,3,4\}} b_i =: \sum_{i\in(4]} b_i =: \sum_{1=1}^{4} b_i \ ;$$

$$c_1 + c_2 + \cdots + c_{10} =: \sum_{j\in(10]} c_j \ .$$

I simboli multiari come $\sum_{i\in I}$ con I insieme numerico, sono particolarmente vantaggiosi quando applicati a operandi caratterizzati da indici appartenenti a I i cui valori sono ottenibili da espressioni dell'indice.
Per esempio se $b_1 = 3, b_2 = 6, b_3 = 0, b_4 = 2$, allora $\sum_{i\in\{1,2,3,4\}} b_i = 11$.
Inoltre accade che $\sum_{h\in(6]} h = 21$ e $\sum_{h\in(6]} h^2 = 91$.
Possono essere utili anche "corse" su insiemi di valori di indici ottenuti con operazioni insiemistiche su intervalli: per esempio

$$\sum_{i\in((6]\cup[9:12]} i \ = \ \sum_{i\in((12]\setminus\{7,8\})} i \ = \ 63 \ .$$

B10 b.03 Diamo ora una definizione del costrutto **sommatoria** applicato a numeri naturali identificati da simboli dotati di un indice variabile in qualche insieme finito di contrassegni, cioè da simboli della forma a_i, con le seguenti richieste.

Per ogni duetto di indici $\{h,k\}$: $\displaystyle\sum_{i\in\{h,k\}} A_i \;:=\; A_h + A_k$.

Per ogni insieme finito I adatto a fornire possibili valori per l'indice e ogni $u \notin I$:

$$\sum_{i\in(I\,\dot\cup\,\{u\})} A_i \;:=\; \sum_{i\in I} A_i + A_u \ .$$

Per poter disporre di un costrutto che si serve di un indice che varia sopra un qualsiasi insieme finito di contrassegni aggiungiamo anche le richieste

$$\sum_{i\in\{j\}} e_i \;:=\; e_j \quad \text{e} \quad \sum_{i\in\emptyset} e_i \;:=\; 0.$$

Conviene segnalare esplicitamente che la possibilità di utilizzare un insieme per la individuazione dei valori che può assumere l'indice è assicurata dalla commutatività e dalla associatività della somma di interi naturali.

B10 b.04 Dalla definizione discendono gli enunciati che seguono.

(1) Per ogni espressione $\mathcal{E}$ che fornisce un insieme finito $S_\mathcal{E}$ si ha: $\quad \sum_{i\in\mathcal{E}} 1 \;=\; |S_\mathcal{E}|$.

Più concisamente abbiamo

(2) $\displaystyle\sum_{i\in I} 1 \;=\; |I|$ per I insieme finito qualsiasi espresso in qualsiasi modo interpretabile.

(3) $\displaystyle\sum_{i\in(\mathrm{n}\,]} k \;=\; n\cdot k$ per n e k interi naturali arbitrari.

(4) Se I e J sono due insiemi disgiunti di contrassegni che forniscono valori per gli indici di variabili numeriche (naturali), vale la decomposizione

$$\sum_{i\in I} n_i \;+\; \sum_{j\in J} n_j \;=\; \sum_{h\in I\,\dot\cup\, J} n_h \ . \tag{4}$$

Questa uguaglianza esprime in forma generale la associatività della somma di interi naturali. Si osserva che essa vale anche per $J=\emptyset$, grazie alla definizione $\displaystyle\sum_{i\in\emptyset} e_i \;:=\; 0$ e $\forall n\in\mathbb{N}\,:\, 0+n=n$.

(5) Se più in generale I e J sono due insiemi con intersezione non necessariamente vuota adatti a fornire valori per gli indici, si ha

$$\sum_{i\in I} n_i + \sum_{j\in J} n_j \;=\; \sum_{h\in I\cup J} n_h + \sum_{h\in I\cap J} n_h \ . \tag{6}$$

B10 b.05 Nelle definizioni dei costrutti di sommatoria gli indici variabili svolgono un ruolo esclusivamente ausiliario, di meri contrassegni: essi possono essere modificati a piacere e per la loro scelta ci si deve preoccupare solo della buona leggibilità delle espressioni trattate e della sintonia con notazioni simili nel contesto.
Questa pura convenzionalità di ogni indice corrente si esprime anche scrivendo

$$\sum_{i\in I} S_i \;=\; \sum_{j\in I} S_j \quad ,$$

dove i e j sono segni ai quali si chiede solo di essere diversi dagli altri segni presenti nell'espressione.

Si può osservare che anche l'insieme I di variabilità di un indice ha carattere ausiliario e potrebbe essere rimpiazzato da un insieme di equivalente valenza espressiva, e in particolare da un insieme con lo stesso cardinale [B08b04].

Una tale sostituzione, contrariamente alla precedente puramente simbolica, richiede di rispettare certe caratteristiche dell'insieme I (ad esempio un ordinamento) le quali in genere dipendono dal contesto e possono richiedere attenzione.

Abbiamo per esempio:

$$\sum_{i\in(10]} a_{20+i} \;=\; \sum_{i\in[21:30]} a_i \;.$$

B10 b.06 Spesso, come abbiamo già visto nei primi esempi, conviene servirsi di indici che variano in intervalli di numeri naturali.
A esempio si incontrano indici i per i quali si chiede $i = 1, 2, ..., n$, ovvero che si caratterizzano con una richiesta della forma $i \in (\mathrm{n}\,]$.
Talora però conviene accostare alla richiesta precedente una richiesta riguardante un indice che corre sullo stesso intervallo che conviene esprimere diversamente, per esempio con la scrittura $j = 0, 1, ..., n$, ovvero con la $j \in [n]$, oppure chiedendo $k = 0, 1, ..., n-1$, cioè con la $k \in [\mathrm{n}\,)$.
In altri casi possono essere più chiarificanti e significativi intervalli comprendenti interi negativi, come per la richiesta $m = -l, -l+1, ... -1, 0, 1, ..., l-1., l$.

Quando l'insieme di variabilità dell'indice è un intervallo di interi naturali può essere conveniente servirsi di notazioni un po' diverse.

$$\sum_{i\in[h:k]} a_i \;=:\; \sum_{i=h}^{k} a_i \;=:\; \sum_{h\le i\le k} \quad \text{per} \quad h,k\in\mathbb{Z}\;. \tag{1}$$

Le tre espressioni precedenti le chiamiamo, risp., **notazione insiemistica della sommatoria**, **notazione con estremi della sommatoria** e **notazione con relazioni per la sommatoria**.

Esse si usano spesso nei casi in cui $h < k$. Se invece, in particolare, $h = k$ le tre espressioni forniscono a_h, mentre se $h > k$ si conviene che forniscano 0, in accordo con la definizione $\sum_{i\in\emptyset} a_i =: 0$.

La sommatoria consente di esprimere facilmente fatti sui multipli dei numeri, per esempio permette di definire

$$(n-h)\cdot k \;:=\; \sum_{i=h+1}^{n} k\;.$$

Una composizione di due sequenze numeriche $\langle a_1, ..., a_n\rangle$ e $\langle b_1, ..., b_n\rangle$ che riveste grande interesse e viene chiamata **convoluzione discreta** si definisce con l'espressione

$$\sum_{i=1}^{n} a_i \cdot b_{n-i}\;.$$

B10 b.07 Ci proponiamo ora di effettuare un'estensione dell'operazione di prodotto analoga alla estensione dell'operazione di somma al costrutto sommatoria, introducendo, in modo simile, il costrutto chiamato **produttoria**.

Qui ci limitiamo a considerare la produttoria applicata a interi naturali con il ruolo di fattori; anche per questi fattori chiediamo che siano forniti da simboli dotati di un indice o anche da espressioni contenenti un indice; denotiamo tali fattori con a_i e chiediamo che l'indice i possa variare in un determinato insieme finito I di contrassegni.

Si avanzano le seguenti richieste.

Per ogni duetto di indici $\{h,k\}$: $\quad \prod_{i\in\{h,k\}} a_i \;:=\; a_h\cdot a_k$

Per ogni insieme di indici J, per ogni $u \in J$ e per ogni $I \subseteq (J \backslash \{u\})$ si ha $\prod_{i \in (I \dot\cup \{u\})} a_i := \left(\prod_{i \in I} a_i\right) \cdot a_u$.

Per poter disporre di un costrutto che si serve di un indice che varia sopra ogni insieme finito di contrassegni aggiungiamo anche le definizioni

$$\prod_{i \in \{j\}} a_i := a_j \quad \text{e} \quad \prod_{i \in \emptyset} a_i := 1.$$

Si osserva anche che la possibilità di utilizzare un insieme per la individuazione univoca dei valori dell'indice è garantita dalla commutatività e dalla associatività del prodotto di interi naturali.

Si ottiene quindi per ogni duetto di insiemi disgiunti di indici I e J

$$\prod_{i \in (I \dot\cup J)} a_i = \left(\prod_{i \in I} a_i\right) \cdot \left(\prod_{j \in J} a_j\right) .$$

Questa formula si dice esprimere la **associatività generalizzata del prodotto**.
Si osserva che essa vale anche per $J = \emptyset$, in forza della richiesta $\prod_{i \in \emptyset} a_i =: 1$.

Più in generale se I e J sono insiemi di indici non necessariamente disgiunti si ha

$$\left(\prod_{i \in I} a_i\right) \cdot \left(\prod_{j \in J} a_i\right) = \left(\prod_{i \in (I \cup J} a_i\right) \cdot \left(\prod_{j \in (I \cap J)} a_j\right) .$$

Anche per la produttoria di fattori individuati da indici che variano in intervallo di interi possono essere convenienti, accanto alle notazioni insiemistiche, le notazioni mediante estremi e le notazioni mediante relazioni.

$$\prod_{i \in [\![h:k]\!]} a_i =: \prod_{i=h}^{k} a_i =: \prod_{h \le i \le k} a_i \qquad \text{per } h, k \text{ interi naturali.}$$

Si osservi che se $h = k$ le tre espressioni forniscono a_h, mentre se $h > k$ si conviene che forniscono 1, in accordo con la $\prod_{i \in \emptyset} a_i := 1$.

La produttoria consente anche di esprimere fatti sulle potenze.
In particolare è compatta e significativa la definizione

$$k^n := \prod_{i=1}^{n} k .$$

B10 b.08 Sono spesso utili costrutti di sommatoria e produttoria che si servono di più indici.

Le più semplici notazioni a due indici si possono introdurre per controllare un insieme di oggetti $a_{i,j}$ associati a coppie appartenenti a un prodotto cartesiano, $\langle i, j \rangle \in I \times J$. Si definisce quindi

$$\sum_{i \in I, j \in J} a_{i,j} := \sum_{\langle i,j \rangle \in I \times J} a_{i,j} . \tag{1}$$

La sommatoria su due indici quindi viene ricondotta a una nota sommatoria su un indice il quale varia in un insieme di coppie costituente un prodotto cartesiano.

Per esempio se $I = \{1, 2\}$, $J = \{1, 2, 3\}$, $a_{1,1} = 3$, $a_{1,2} = 5$, $a_{1,3} = 0$, $a_{2,1} = 4$, $a_{2,2} = 3$, $a_{2,3} = 1$, si ottiene $\sum_{i \in I, j \in J} a_{i,j} = 16$, mentre $\sum_{i \in I, j \in J} i \cdot 2^j = 42$.

Definizioni simili si introducono per il prodotto; in particolare la omologa della formula (1) è

$$\prod_{i\in I, j\in J} a_{i,j} \;:=\; \prod_{\langle i,j\rangle\in I\times J} a_{i,j}\ . \tag{2}$$

La sommatoria su due indici consente di esprimere concisamente la proprietà che viene chiamata **distributività generalizzata di somma e prodotto** per i numeri interi.

$$\left(\sum_{i\in I} a_i\right)\cdot\left(\sum_{j\in J} b_j\right) \;=\; \sum_{\langle i,j\rangle\in(I\times J)} a_i\cdot b_j\ . \tag{3}$$

Essa evidentemente estende le due uguaglianze che esprimono la distributività

$$(a+b)\cdot c = a\cdot c + b\cdot c \qquad , \qquad (a+b)\cdot(c+d) = a\cdot c + b\cdot c + a\cdot d + b\cdot d\ .$$

B10 b.09 Ragruppamenti più elaborati si rendono necessari quando tra i due indici si impongono vincoli e condizionamenti.

Una sommatoria come la seguente vede la coppia dei due indici muoversi su un insieme "triangolare" di 485 coppie di interi positivi:

$$\sum_{1\le i\le j<24} a_{i,j}\ .$$

Sono coinvolti gli addendi associati a un triangolo più ridotto, di 442 di coppie di interi maggiori di 1 nella sommatoria che segue:

$$\sum_{1<i<j<24} (a_{i,j} + 2\,b_{i,j})\ .$$

Il prodotto dei numeri $a_{i,j}$ che sono stati associati alle sole caselle bianche della scacchiera è fornito dall'espressione:

$$\prod_{i\in(8]\wedge j\in(8]\wedge(i+j=_2 0)} a_{i,j}\ .$$

Possono essere spesso utili anche composizioni che richiedono tre indici: la somma di certi numeri associati ai cubetti che compongono un cuboide discreto si ottengono con espressioni della forma seguente:

$$\sum_{i\in I}\sum_{j\in J}\sum_{h\in\mathsf{H}} (a_{i,j,h} - 2\,b_{i,2j})\ .$$

Queste composizioni si possono descrivere ricorrendo alla geometria di quello che possiamo chiamare "spazio Lego", spazio nel quale si possono collocare mattoncini che per semplicità pensiamo cubici; la seguente sommatoria riguarda addendi collocabili nei mattoncini cubici che formano una piramide a base quadrata:

$$\sum_{i=1,\ldots,20}\ \sum_{j=1,\ldots,20}\ \sum_{h=1,\ldots,21-\min(i,j,21-i,21-j)} (c_i - 2d_j + 3e_h)\ .$$

Segnaliamo che possono rivestire grande interesse anche sommatorie e produttorie su indici il cui numero viene lasciato indeterminato come nella seguente espressione:

$$\sum_{i_1,i_2,\ldots,i_h=1,2\ldots,m} a_{i_1,i_2,\ldots,i_h}\ .$$

Una tale espressionepuò essere meglio compresa associando i suoi addendi a punti di un ipercubo nello spazio di h dimensioni.

B10 c. somma di naturali mediante notazioni posizionali

B10 c.01 Vediamo ora come si può procedere per effettuare le operazioni di somma e prodotto di interi naturali operando sulle relative scritture posizionali in una database $B = 2, 3, 4, ..., 8, 9, 10, ..., 16, ...$.

Cominciamo con l'osservare che interessano principalmente le operazioni su numeri interi positivi, in quanto in presenza di un operando nullo il risultato è fornito dalle semplici formule $m + 0 = m$ e $n \cdot 0 = 0$. Tuttavia non è possibile non occuparsi dello 0 che può essere messo in gioco da operazioni come $2 \cdot 5 = 10$.

Si comincia con l'osservare che la sommatoria consente di esprimere concisamente e con generalità le decomposizioni degli interi positivi nelle varie basi B:

$$\sum_{i=0}^{q} c_i \cdot B^i \;=\; c_q \cdot B^q + c_{q-1} \cdot B^{s-1} + \cdots + c_1 \cdot B + c_0 \; . \tag{1}$$

In generale consideriamo gli interi positivi $m := \sum_{i=0}^{h} c_i \cdot B^i$ e $n := \sum_{i=0}^{k} d_i \cdot B^i$ con $0 \le h, k$, $0 \le c_h, d_k < B$ e $0 < c_h, d_k < B$. Ci poniamo il problema di trovare la notazione in base B della loro somma $m + n =: \sum_{i=1}^{t} s_i \cdot B^i$ con $0 \le s_i < B$ per $i \in [1 : t)$ e $0 < s_t < B$.

Al fine di semplificare le espressioni dei calcoli denotiamo con u il maggiore dei due esponenti massimi delle basi aumentato di 1 e introduciamo coefficienti c_i o d_i nulli in modo di trattare con due sequenze di cifre in base B aventi la stessa lunghezza u: definiamo quindi $c_j := 0$ per $h < j \le u$ e $d_j := 0$ per $k < j \le u$.

Possiamo allora scrivere per le

$$\begin{aligned} m + n \;&=\; \sum_{i=0}^{u} c_i \, B^i + \sum_{i=0}^{u} d_i \, B^i \;=\; \sum_{i=0}^{u} (c_i + d_i) \, B^i \\ &= 0 \cdot B^u + (c_{u-1} + d_{u-1}) B^{u-1} + \cdots + (c_2 + d_2) \cdot B^2 + (c_1 + d_1) \cdot B + (c_0 + d_0) \; . \end{aligned} \tag{2}$$

Questa scrittura mostra che sul coefficiente s_0 della somma può influire solo $c_0 + d_0$, in quanto ciascuno degli altri addendi dà un multiplo di B. Più in generale sul coefficiente s_i della espressione cercata possono influire solo le somme $c_j + d_j$ con $j \le i$, in quanto gli addendi più a sinistra (cioè più pesanti) forniscono come contributo un multiplo di B^{i+1}. Quindi occorre procedere a calcolare nell'ordine s_0, s_1, ..., s_t.

Se tutte le somme $c_i + d_i$ sono inferiori a B, il calcolo complessivo si riduce a effettuare separatamente le somme di coefficienti. Spesso invece qualche $c_i + d_i$ è maggiore di $B - 1$; tale valore non può comunque superare $2B - 2$.
In questi casi è necessario aggiungere un addendo 1, chiamato **riporto**, alla somma dei coefficienti della potenza B^{i+1}. Si hanno quindi somme di due coefficienti a ciascuna delle quali si può aggiungere un eventuale riporto procedendo per valori dell'indice i da 1 in su; ribadiamo che nessuna di queste somme può superare $2B - 1$, quindi il riporto al crescere dell'indice i, cioè procedendo da destra a sinistra, non può che valere 0 o 1.

B10 c.02 Le considerazioni precedenti conducono al seguente schema di calcolo:

$$s_0 = (c_0 + d_0) \,\%\, B; \qquad\qquad r_1 := (c_0 + d_0) : B;$$

$$\begin{array}{ll} s_1 = (r_1 + c_1 + d_1)\,\%\,B; & r_2 := (r_1 + c_1 + d_1) : B; \\ \cdots\cdots & \cdots\cdots \\ s_i = (r_i + c_i + d_i)\,\%\,B; & r_{i+1} := (r_i + c_i + d_i) : B; \\ \cdots\cdots & \cdots\cdots \\ s_{u-1} = (r_{u-1} + c_{u-1} + d_{u-1})\,\%\,B; & r_u := (r_{u-1} + c_{u-1} + d_{u-1}) : B \end{array}$$

In particolare facciamo riferimento alla base $B = 10$ e applichiamolo alla somma $687 + 2955$. In questo caso abbiamo $u = 3$ e

$$\begin{array}{ll} s_0 := 12\,\%\,10 = 2; & r_1 = 12 : 10 = 1; \\ s_1 := (1 + 8 + 5)\,\%\,10 = 14\,\%\,10 = 4; & r_2 = 14 : 10 = 1; \\ s_2 := (1 + 6 + 9)\,\%\,10 = 16\,\%\,10 = 6; & r_3 = 16 : 10 = 1; \\ s_3 := (1 + 0 + 2)\,\%\,10 = 3\,\%\,10 = 3; & r_4 = 3 : 10 = 0; \end{array}$$

L'ultimo risultato dice che questa somma ha una rappresentazione decimale avente lunghezza uguale alla massima delle lunghezze degli addendi. Abbiamo quindi $687 + 2955 = 3642$.
Se invece si considera $687 + 9955$ bisogna modificare le ultime operazioni nelle

$s_3 = (1 + 0 + 9)\,\%\,10 = 10\,\%\,10 = 0; \qquad r_4 = 10 : 10 = 1$.

Quindi si ha $687 + 9\,955 = 10\,642$, numero con una rappresentazione decimale avente lunghezza pari alla lunghezza dell'addendo maggiore aumentata di 1, dovuta al fatto che l'ultimo resto è uguale a 1.

Questo esempio e le considerazioni del paragrafo precedente costituiscono indicazioni sufficienti per la effettuazione del calcolo della somma di due interi positivi qualsiasi mediante le loro rappresentazioni in base B.

B10 c.03 Se si conviene di porre $r_0 := 0$, lo schema per il calcolo della somma di due interi positivi si può mettere sotto la seguente forma compatta.

$$\begin{array}{l} r_0 := 0; \\ \text{per} \;\; i = 0, ..., u \;\; : \;\; \left\{ \; s_i := (r_i + c_i + d_i)\,\%\,B \; ; \;\; r_{i+1} := \left\lfloor \dfrac{r_i + c_i + d_i}{B} \right\rfloor \right\} \; ; \\ s_{u+1} := r_{u+1}; \end{array} \tag{1}$$

Da queste formule si vede che l'esecuzione di questi calcoli richiede manovre locali che si riducono alla espressione in base B della somma di due numeri inferiori a B e al suo eventuale aumento di 1 (operazione vista in c01]. Si osserva inoltre che il complesso di queste manovre locali può essere organizzato in modo abbastanza semplice, ma non banale.
Si spiegano quindi le difficoltà incontrate nell'apprendimento di questa tecnica, fondamentale per imparare a "fare di conto", ma spesso fonte di ostilità di fronte all'aritmetica (e successivamente della matematica) di chi si sente costretto a memorizzare le manovre sopra esposte senza l'aiuto del loro significato.

Questo procedimento di calcolo viene insegnato a tutti i futuri cittadini e dovrebbe essere messo in pratica: per approppriarsene l'esecutore dovrebbe rendersi conto della sensatezza delle rappresentazioni in base B delle operazioni $h + k$ per $h, k = 0, 1, 2, ..., B - 1$ e del fatto che sono state una faticosa conquista culturale (mentale e sociale).

Va segnalato anche che la attuale disponibilità dei dispositivi elettronici per il calcolo induce a giudicare inutile la comprensione di queste manovre, elemento da considerare un contributo alla poca comprensione delle presenze tecnologiche nella società attuale, con il rischio della passività nei confronti delle innovazioni che ci crescono intorno.

B10 c.04 Le informazioni da gestire per sommare due interi positivi (e non solo) si possono organizzare in una tabella quadrata di B linee orizzontali e B linee verticali da porre in corrispondenza con i numeri 0, 1, ..., $B-1$, chiamata **tavola di composizione per la somma in base** B.

Nel caso usuale $B = 10$ la tavola di composizione della somma viene presentata nella forma nota della scuola primaria come "tabellina della somma":

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	3	4	5	6	7	8	9	10	11
3	3	4	5	6	7	8	9	10	11	12
4	4	5	6	7	8	9	10	11	12	13
5	5	6	7	8	9	10	11	12	13	14
6	6	7	8	9	10	11	12	13	14	15
7	7	8	9	10	11	12	13	14	15	16
8	8	9	10	11	12	13	14	15	16	17
9	9	10	11	12	13	14	15	16	17	18
10	10	11	12	13	14	15	16	17	18	19

Il suo contenuto può essere ricostruito facilmente; per questo strumento computazionale si sono potute utilizzate le dita delle mani e si è fatto ricorso a vari strumenti materiali.
In effetti si tratta di una manovra di grande importanza per la storia dell'uomo e delle società, in quanto da alcuni secoli ha potuto essere praticata ampiamente e vantaggiosamente.

B10 c.05 La relativa semplicità dello schema della somma ha consentito anche la costruzione di apparecchiature digitali che hanno effettivamente aiutato molto l'esecuzione dei calcoli numerici, a partire da quelli sugli interi.

Fin dall'antichità sono stati adottati dispositivi come l'`abaco (wi)` nel quale piccoli oggetti possono essere mossi in scanalature o come sistemi di corde opportunamente annodate.

Nei secoli XVI e XVII sono state costruite le prime macchine calcolatrici (da Wilhelm Schickard , Blaise Pascal e Gottfried Leibniz); queste si servivano di ruote dentate e del dispositivo per la gestione dei riporti chiamato nottolino.

Si è tuttavia dovuto attendere la meccanica di precisione dell'inizio del XIX secolo per disporre di calcolatrici meccaniche di ampia diffusione (Thomas de Colmar); intorno all'inizio del XX secolo si è sviluppata la tecnologia elettromeccanica che ha rese disponibili le calcolatrici elettromeccaniche e negli anni 1940 si sono cominciati ad utilizzare i calcolatori elettronici mentre negli anni intorno al 1970 si è avuta la diffusione capillare delle calcolatrici elettroniche. Tutto questo ha rapidamente soppiantato in buona parte le precedenti pratiche di calcolo eseguito dalle persone.

A proposito di calcolo elettronico va osservato che La tavola di composizione della somma è particolarmente semplice per le rappresentazioni binarie, cioè per la base $B = 2$.

	0	1
0	0	1
1	1	10

Dato che anche l'esecuzione delle scelte sopra disuguaglianze numeriche complessiva dei calcoli è notevolmente semplice per le rappresentazioni binarie si è giunti alla realizzazione di dispositivi binari di elevatissima velocità, basso consumo e alta attendibilità della attuale tecnologia informatica.

B10 c.06 (1) Eserc. Costruire le tavole di composizione per la somma nelle basi 3, 5, 7, 16.

(2) Eserc. Eseguire le seguenti somme:

$1111111_2 + 1111111_2 \qquad 11111111_2 + 1_2$
$1234_5 + 4321_5 \qquad 1234_6 + 4321_6$
$111111111111_2 + 111111_4 + 1111_8$
$121212_4 + 121212_8$
$1020102_3 + 1212_9$

B10 c.07 In molte attività pratiche (amministrazione, finanza, commercio al minuto e all'ingrosso, arredamento di interni, conteggi in laboratorio, ...) accade di dover sommare parecchi interi positivi. Questo problema può formalizzarsi con le seguenti espressioni

(1) Dati A addendi in notazione posizionale $n_a = \sum_{i=0}^{h_a} c_{a,i} B^i$ per $a = 1, 2, ..., A$

$$\text{calcolare} \quad \sum_{a=1}^{A} n_a =: \sum_{i=0}^{t} s_i \, B^i \quad \text{con} \quad s_i \in [B) \ \text{ per } \ i = 0, 1, ..., t-1 \ \text{ e } \ s_t \in (B) \ .$$

Si tratta di ridurre all'ultima espressione lo sviluppo, ottenuto inserendo opportuni coefficienti $c_{a,j}$ assunti nulli, e con $u := \min(h_1, ..., h_A)$.

(2) $$\sum_{i=0}^{u} \left(\sum_{a=1}^{A} c_{a,i} \right) B^i \ .$$

Il problema è quindi un'estensione del problema della somma di due numeri risolvibile con lo schema di calcolo in c02 e c03.

Questo problema può risolversi riconducendolo ad $A-1$ somme di interi; questo è quello che viene fatto dalle calcolatrici numeriche e dai programmi di calcolo numerico nei linguaggi procedurali (Fortran, C++, Java, ...) o nei sistemi per i calcoli numerici, grafici e simbolici (MatLab, Maple, Mathematica, Octave, ...).

Nei calcoli manuali risulta più conveniente adottare uno schema di calcolo che estende c03(1) esprimibile come segue:

(3) $$r_0 := 0; \quad \text{per} \quad i = 0, ..., u \ : \quad \left[\ s_i := \left(r_i + \sum_{a=1}^{A} c_{a,i} \right) \% \, B \ ; \quad r_{i+1} := (r_i + c_i + d_i) : B \ \right] \ .$$

Questo schema rispetto al precedente richiede in più solo di applicare più volte la tabella di composizione per la somma e il passaggio all'intero successivo e di ricordare riporti che possono essere superiori a 1 e potrebbero richiedere anche più cifre.

B10 d. prodotto e quoziente di naturali mediante notazioni posizionali

B10 d.01 Poniamoci ora il problema di trovare la scrittura in una qualsiasi base $B = 2, 3, 4, ...$ del prodotto di due interi positivi che scriviamo

$$m := \sum_{i=0}^{h} c_i \cdot B^i \quad \text{ed} \quad n := \sum_{i=0}^{k} d_i \cdot B^i \qquad \text{con} \quad 0 \leq h, k \ \text{ e } \ 0 \leq c_h, d_k < B \ .$$

Si tratta di un calcolo più complesso del precedente che può realizzarsi in maniere diverse.
Anch'esso comunque si può effettuare organizzando manovre piuttosto semplici sui coefficienti delle notazioni posizionali dei due operandi.
Noi ci serviremo di un rimaneggiamento della espressione per il prodotto che utilizza la distributività del prodotto rispetto alla somma, cioè l'uguaglianza

$$m \cdot n \ = \ \sum_{j=0}^{k} \left(\sum_{i=0}^{h} c_i \cdot B^i \right) \cdot d_j \cdot B^j \ .$$

Essa si riduce alla seguente somma di interi

$$m \cdot n \ = \ \sum_{j=0}^{k} Q_j \cdot B^j \ ,$$

nella quale intervengono i numeri, che chiameremo intermedi, dati dall'espressione

$$Q_j \ := \ \left(\sum_{i=0}^{h} c_i \cdot B^i \right) \cdot d_j \ = \ \sum_{i=0}^{h} (c_i \cdot d_j) \cdot B^i \ = \ c_h \cdot d_j \cdot B^h + \cdots + c_1 \cdot d_j \cdot B + c_0 \cdot d_j \ .$$

Il calcolo di questi numeri nella rappresentazione in base B, che scriviamo $Q_j = \sum_{i=0}^{t} q_{i,j} \cdot B^j$, somiglia molto a quello della somma in c01 . Ancora si hanno coefficienti di potenze di B che possono essere maggiori di $B - 1$, e quindi si pongono problemi di riporto; ancora nel calcolo della rappresentazione in base B bisogna procedere per coefficienti di potenze crescenti, visivamente sui coefficienti da destra a sinistra; ancora i riporti sono contenuti e si ottengono numeri non superiori a

$$(B-1) \cdot (B-1) + (B-1) \ = \ B \cdot (B-1) \ .$$

Si trova quindi che i coefficienti $q_{i,j}$ si ottengono seguendo il seguente schema di calcolo:

$$\begin{array}{cc}
q_{0,j} := (c_0 \cdot d_j) \,\%\, B; & r_{1,j} := (c_0 \cdot d_j) : B; \\
q_{1,j} := (r_{1,j} + c_1 \cdot d_j) \,\%\, B; & r_{2,j} := (r_{1,j} + c_1 \cdot d_j) : B; \\
\cdots\cdots\cdots & \cdots\cdots\cdots \\
q_{i,j} := (r_{i,j} + c_i \cdot d_j) \,\%\, B; & r_{i+1,j} := (r_{i,j} + c_i \cdot d_j) : B; \\
\cdots\cdots\cdots & \cdots\cdots\cdots \\
q_{u-1,j} := (r_{u-1,j} + c_{u-1} \cdot d_j) \,\%\, B; & r_u := (r_{u-1,j} + c_{u-1} \cdot d_j) : B
\end{array}$$

B10 d.02 Ancora servono le conoscenze dei risultati di una composizione di due interi appartenenti a $[B)$: ora si tratta di conoscere le rappresentazioni in base B dei prodotti $f \cdot g$ con $f, g \in [B)$.

Quindi è necessario conoscere, oltre alla tavola di composizione per la somma che serve alla valutazione della somma complessiva, una tavola corrispondente ma relativa ai prodotti, avente linee orizzontali e verticali corrispondenti ai numeri 0, 1, ..., $B - 1$, chiamata **tavola di composizione per il prodotto in base** B.

Nel caso $B = 10$ si ottiene la tavola di composizione per il prodotto che di solito viene presentata nella forma che segue e viene chiamata "tabellina del prodotto".

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	27	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50
6	6	12	18	24	30	36	42	48	54	60
7	7	14	21	28	35	42	49	56	63	70
8	8	16	24	32	40	48	56	64	72	80
9	9	18	27	36	45	54	63	72	81	90
10	10	20	30	40	50	60	70	80	90	100

B10 d.03 Si tratta poi di effettuare i calcoli che riducono l'espressione

$$m \cdot n \;=\; \sum_{j=0}^{k} Q_j \cdot B^j \;=\; \sum_{j=0}^{k} \left(\sum_{i=0}^{t} q_{i,j} \cdot B^j \right) B^j$$

alla forma

$$\sum_{i=0}^{v} s_i B^i \quad \text{con} \quad s_i \in [\![B]\!) \;\text{ per }\; i = 0, 1, ..., v-1 \quad \text{e} \quad s_v \in (\![B]\!) \;.$$

L'espressione da ridurre riguarda la somma di k interi positivi $Q_j \cdot B^j$ aventi rappresentazioni in base B ottenute accodando alle rappresentazioni $q_{v,j}\, q_{v-1,j} \cdots q_{1,j}\, q_{0,j}$ una sequenza di j zeri (per $j = 0, 1, ..., k$). Questa operazione è stata presentata in c07 .

Resta solo da aggiungere che il calcolo manuale di una somma del tipo precedente conviene sia organizzata disponendo le cifre $q_{i,j}$ in un cosiddetto "parallelogramma-ZZ", in modo da avere incolonnati i coefficienti relativi allo stesso $i + j$, come esemplificato dalla seguente disposizione riguardante $v = 4$ e $k = 3$.

$$\begin{array}{cccccc}
 & & q_{4,0} & q_{3,0} & q_{2,0} & q_{1,0} & q_{0,0} \\
 & q_{4,1} & q_{3,1} & q_{2,1} & q_{1,1} & q_{0,1} & \\
q_{4,2} & q_{3,2} & q_{2,2} & q_{1,2} & q_{0,2} & & \\
q_{4,3} & q_{3,3} & q_{2,3} & q_{1,3} & q_{0,3} & &
\end{array}$$

B10 d.04 I calcoli per i numeri in notazione binaria sono particolarmente semplici. In questo caso per ottenere i numeri intermedi basta riportare il primo fattore opportunamente completato con zeri solo per i coefficienti d_j uguali ad 1.

Per esempio per il prodotto $101101_2 \cdot 1001_2$ si ha la disposizione seguente

$$\begin{array}{cccccccc}
 & & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
 & & & & 1 & 0 & 0 & 1 & 1 \\
 & & — & — & — & — & — & — & — \\
 & & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & & \\
— & — & — & — & — & — & — & — & — \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1
\end{array}$$

B10 d.05 **(1) Eserc.** Scrivere le tavole di composizione del prodotto nelle basi 4, 5 e 8.

(2) Eseguire i seguenti prodotti

$1111111_2 \cdot 1111111_2 \qquad 11111111_2 \cdot 1_2$
$1234_5 \cdot 4321_5 \qquad 1234_6 \cdot 4321_6$
$111111111111_2 \cdot 111111_4 \cdot 1111_8$
$121212_4 \cdot 121212_8$
$1020102_3 \cdot 1212_9$

B10 d.06 Dati due interi positivi m ed n attraverso le loro notazioni in una base B

$$Ntn_B(m) \;=\; \sum_{i=0}^{h} a_i\, B^i \quad \text{e} \quad Ntn_B(n) \;=\; \sum_{j=0}^{k} b_j\, B^j \;,$$

è facile decidere se $m < n$, oppure $m = n$ oppure $m > n$.

Se $h < k$ si decide che $m < n$, mentre se $h > k$ si conclude che $m > n$.
Nel caso sia $h = k$ si corre sulle coppie di coefficienti $\langle a_i, b_i \rangle$ per $i = h, h-1, ..., 1, 0$, cioè da sinistra a destra, ovvero dalle cifre più pesanti alle più leggere, e si confrontano i due valori.
Nella fase relativa alla potenza B^i se $a_i < b_i$ si decide che $m < n$, mentre se $a_i > b_i$ si conclude che $m > n$; in entrambi questi casi si interrompe la corsa, mentre se $a_i = b_i$ si procede alla fase relativa all'indice $i - 1$.
Se la corsa si conclude dopo aver verificato che $a_0 = b_0$, e solo in questo caso, cioè sse le duenotazioni coincidono, si conclude che $m = n$.

B10 d.07 Poniamoci ora il problema di individuare le notazioni in base B del quoziente $q = \sum_{i=0}^{t} c_i\, B^i$ e del resto r tra due interi positivi m ed n dati attraverso le notazioni posizionali nella base B

$$Ntn_B(m) \;=\; \sum_{i=0}^{h} a_i\, B^i \quad \text{e} \quad Ntn_B(n) \;=\; \sum_{j=0}^{k} b_j\, B^j \;.$$

Se si trova $m < n$ il problema si risolve subito fornendo $q = 0$ e $r = n$.

In caso contrario consideriamo innanzi tutto il caso relativamente semplice in cui $h = k$: in tal caso deve essere $1 \le q \le B - 1$ e si tratta di individuare il minimo multiplo di n $\overline{q} \in [1 : B]$ che supera m, operazione che richiede di effettuare prodotti [d03] e confronti [d06] e che potrebbe essere conveniente facilitare predisponendo la tabella delle notazioni in base B dei $B-1$ multipli di n $2\,n$, $3\,n$,...,$(B-1)n$.

Trovato il richiesto $\overline{q}$ si conclude che $q = \overline{q} - 1$ e infine si calcola il resto $r = m - q \cdot n$ attraverso una differenza (simile alla somma) e un prodotto.

Se accade, più in generale, che $h > k$ può essere necessaria una corsa volta a determinare le diverse cifre c_i di $Ntn_B(q)$ a partire da quella più pesante.

Nel caso che sia $h = k + 1$ e $m < B \cdot n$ ancora $Ntn_B(q)$ consiste in una sola cifra in base B che si determina come nel caso $h = k$ con la sola complicazione di confronti di notazioni su $k + 2$ cifre invece che su $k + 1$. Se $m \ge B \cdot n$ o $h > k + 1$ si deve procedere secondo lo schema che segue.

Inizialmente si pone provvisoriamente $t := 0$ e si introduce una notazione in base B ausiliaria σ che nella corsa che si sta avviando si andrà modificando e alla fine fornirà $Ntn_B(r)$.
Si pone poi $\sigma := \sum_{j=h,\ldots,h-k} a_j\, B^{j-h+k}$ se tale numero è maggiore o uguale a n, mentre in caso contrario a σ si assegna una cifra ponendo $\sigma := \sum_{j=h,\ldots,h-k-1} a_j\, B^{j-h+k+1}$.
Poniamo $t := h - k$ nel primo caso e $t := h - k - 1$ nel secondo.

In entrambi i casi σ si può esprimere con $\sigma = n \cdot c_t + r_0$, con $c_t := (\sigma \preceq_: n) \in [1 : B)$ ed $r_0 := \sigma \,\%\, n$.
Si è quindi trovato che $m = n \cdot c_t \cdot B^t + r_0 \cdot B^t + M \,\%\, B^t$ e il problema viene ricondotto al calcolo di quoziente e resto tra $m_{t-1} := r_{t-1} \cdot B^t + m \,\%\, B^t$ ed n, quoziente sicuramente minore di B^t.
Il calcolo procede attraverso stadi simili a quella iniziale che ha condotto a c_t, stadi che conducono successivamente alle cifre c_{t-1}, ... , c_1 e c_0 .
Nell'u-esimo di questi stadi, con $u = t-1, ..., 1, 0$ si considera una frazione σ_u/n con $\sigma_u := r_u \cdot B + a_u$ e si individuano $c_u := \left\lfloor \frac{\sigma_u}{n} \right\rfloor \in [0 : B)$ ed $r_{u-1} := \sigma_u \,\%\, n \in [0 : n)$.
Con l'ultima fase si individuano $c_0 := \left\lfloor \frac{\sigma_0}{n} \right\rfloor$ e $r_0 = \sigma_0 \,\%\, n$, cioè la cifra più a destra di $Ntn_B(q)$ e il resto $m \,\%\, n$.

B10 d.08 Vediamo come si sviluppano alcuni calcoli di quoziente e resto nella base 10.

$$\frac{273}{125} = \frac{2 \cdot 125 + 23}{125} = 2 + \frac{23}{125}$$

$$\frac{4278}{125} = \frac{427}{125} \cdot 10 + \frac{8}{125} = \frac{3 \cdot 125}{125} \cdot 10 + \frac{103}{125} \cdot 10 + \frac{8}{125} = 3 \cdot 10 + \frac{1038}{125} = 3 \cdot 10 + \frac{8 \cdot 125 + 38}{125} = 38 + \frac{38}{125}$$

$$\frac{45072}{23} = \frac{45}{23} \cdot 10^3 + \frac{72}{23} = 1 \cdot 10^3 + \frac{22 \cdot 10 + 0}{23} \cdot 10^2 + \frac{72}{23} = 1 \cdot 10^3 + \frac{23 \cdot 9 + 13}{23} \cdot 10^2 + \frac{72}{23} =$$

$$19 \cdot 10^2 + \frac{137}{23} \cdot 10 + \frac{2}{23} = 19 \cdot 10^2 + \frac{23 \cdot 5 + 22}{23} \cdot 10 + \frac{2}{23} = 195 \cdot 10 + \frac{222}{23} = 195 \cdot 10 + \frac{23 \cdot 9 + 15}{23} = 1959 + \frac{15}{23}$$

B10 d.09 Un'altra manovra che riveste interesse riguarda la trasformazione della notazione di un intero positivo in una prima base B, $n = \sum_{i=0}^{k} b_i \, B^i$ nella notazione in una seconda base C, $n = \sum_{i=0}^{t} c_i \, C^i$.
Questa manovra può effettuarsi anche servendosi solo delle notazioni, ma la sua descrizione risulta assai pesante in quanto si devono distinguere casi come i seguenti: $B < C < B^2$, $C = B^2$, $B^2 < C < B^3$, $C = B^3$, $B^3 < C < B^4$ e quelli in cui B e C si scambiano i ruoli.

Ci limitiamo a osservare che nel caso sia $C = B^h$ con $h = 2, 3, ...$ il cambiamento di base richiede soltanto di trasformare h cifre consecutive in base B in una notazione in base C procedendo dai coefficienti meno pesanti ai più pesanti.
Se invece $B = C^h$ si ha una transcodifica che consiste nel trasformare ogni cifra in base B in h cifre in base C (come nei casi visti in a10).

Questa manovra di transcodifica, come altre manovre, si semplifica se si dispone della possibilità di trattare gli interi con una codifica interna con la quale si possono effettuare le varie operazioni, come accade con gli usuali linguaggi di programmazione procedurali, almeno fino a che si trattano interi che non superano un limite accettabile per gran parte delle esigenze, per esempio interi positivi con valori inferiori a 2^{31}.
In questi casi si possono effettuare tutte le operazioni con questi strumenti e giungere alle codifiche finali con il meccanismo relativamente semplice dell'individuazione delle successive cifre nella base richiesta, procedendo dalle meno pesanti alle più pesanti.
Nel caso del cambiamento dalla base B alla C si tratta di individuare il numero n nella codifica interna eseguendo le operazioni indicate dall'espressione $n = \sum_{i=0}^{k} b_i \, B^i$ e quindi di individuare le cifre c_i con la seguente sequenza di passi

$n + 0 := n$; $c_0 := n_0 \,\%\, C$; $n_1 := n_0 : C$; $c_1 := n_1 \,\%\, C$; $...c_{t-1} := n_{t-1} \,\%\, C$; $n_t := n_{t-1} : C$; $c_t := n_t$

dove t viene individuato dalla richiesta che $n_t \in [1 : C)$.

B10 e. produttoria cartesiana di insiemi finiti

B10 e.01 Anche l'operazione binaria prodotto cartesiano di liste e di insiemi si può estendere alla composizione multiaria di più liste o di più insiemi.

Si abbia una sequenza di lunghezza m di insiemi finiti $\mathsf{E} = \langle E_1, E_2, ..., E_m \rangle$ e denotiamo con n_i il cardinale di E_i per ogni $i \in \{1, 2, ..., m\}$.
Si dice prodotto cartesiano della E l'insieme delle m-uple $\langle a_1, a_2, ..., a_m \rangle$ dove per ogni $i = 1, 2, ..., m$ sia $a_i \in E_i$.
Questo insieme si denota con ciascuna delle notazioni seguenti

$$\mathbf{X}_{i=1}^{m} E_i \;=\; \mathbf{X}_{i\in[1:m]} E_i \;=\; \mathbf{X}_{i=1,2,...,m} E_i \ .$$

Questa costruzione viene detta **produttoria cartesiana** e il segno $\mathbf{X}$ viene deto "simbolo della produttoria cartesiana".

Si constata che l'insieme delle notazioni decimali degli interi compresi tra 100 e 999, estremi inclusi, si può esprimere come $\mathbf{X}_{i=1}^{3} E_i$ dove $E_1 := \{1, 2, ..., 9\}$ ed $E_2 := E_3 := \{0, 1, 2, ..., 9\}$.

Abbiamo visto come le terne $\langle a_1, a_2, a_3 \rangle$ si possano identificare con le entità della forma $\big\langle \langle a_1, a_2 \rangle, a_3 \big\rangle$ e con quelle della forma $\big\langle a_1, \langle a_2, a_3 \rangle \big\rangle$; questa identificazione conduce a considerare il prodotto cartesiano un'operazione binaria associativa.

B10 e.02 La produttoria cartesiana si può estendere alle sequenze di insiemi (finiti) le cui posizioni sono individuate da sequenze di indici che possono essere diverse dagli intervalli di numeri positivi degli esempi precedenti.

Se si considera la sequenza di segni $J = \langle j_1, j_2, ..., j_m \rangle$ e se per $h = 1, 2, ..., m$ consideriamo gli insiemi finiti E_{j_h}, definiamo **produttoria cartesiana della sequenza di insiemi** $\langle E_{j_1}, E_{j_2}, ..., E_{j_m} \rangle$, cioè l'insieme di tutte le m-uple della forma $\langle a_{j_1}, a_{j_2}, ..., a_{j_m} \rangle$, dove per ogni $h = 1, 2, ..., m$ si ha $a_{j_h} \in E_{j_h}$.

Tale insieme è finito e si denota con le notazioni equivalenti

$$\mathbf{X}_{h=1}^{m} E_{j_h} \;=\; \mathbf{X}\{j \in\!\!\to J :|\ E_j\} \ .$$

Qui la scrittura $j \in\!\!\to J$ intende esprimere lo scorrimento della sequenza J di contrassegni, operazione più definita di una corsa su un insieme, in quanto il prodotto cartesiano non è commutativo e l'ordine di scorrimento della sequenza deve essere rispettato.

Si osserva che la definizione consente che due insiemi E_{j_1} e E_{j_2} con $j_1 \neq j_2$ possano coincidere, e che la sequenza J può presentare componenti ripetute.

B10 e.03 Possono essere chiarificanti le seguenti uguaglianze.

$$\mathbf{X}_{i=1}^{2} E_i \;=\; E_1 \times E_2 \quad \text{e} \quad \mathbf{X}_{i=1}^{1} E_i \;=\; E_1 \ .$$

Conviene inoltre convenire che nel caso la sequenza di insiemi abbia lunghezza 0 sia

$$\mathbf{X}_{i\in\to\emptyset} E_1 \;:=\; \sqcup \ .$$

Questa scelta consente di formulare la seguente uguaglianza.

$$\mathbf{X}_{j\in\to(J_1\,,\,J_2)} E_j \;=\; \big(\mathbf{X}_{j\in\to J_1} E_j\big) \times \big(\mathbf{X}_{j\in\to J_2} E_j\big) \ ,$$

dove J_1 e J_2 denotano due sequenze di indici ciascuno dei quali, lo scriviamo j, individua uno degli insiemi che scriviamo E_j.

Per il cardinale degli insiemi individuati da una produttoria cartesiana si constata che

$$\left|\mathbf{X}_{j=j_1,j_2,\ldots,j_m}\ E_j\right| \ = \prod_{j=j_1,j_2,\ldots,j_m} |E_j| \ .$$

Nel caso di una sequenza costituite da m repliche dello stesso insieme E abbiamo il cardinale $|E|^m$.
Da questo seguono varie proprietà delle potenze degli interi naturali; in particolare si ha .

$$\left|\mathbf{X}_{j\in\emptyset}\ E_j\right| \ = \ \prod_{j\in\emptyset} |E_j| \ = \ |\emptyset| \ = \ 1 \ .$$

Testo fruibile in https://www.mi.imati.cnr.it/alberto/ e https://arm.mi.imati.cnr.it/Matexp/matexp_main.php