

SCRITTURA DEI NUMERI NATURALI IN UNA BASE ARBITRARIA

(p. 21, Dispense)

DEF. 8.1 Sia $b \in \mathbb{N}$. Diciamo che un numero naturale $n \in \mathbb{N}$ è RAPPRESENTABILE

IN BASE b se esistono $k \in \mathbb{N}$ e $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_k \in I_b$ t.c.

$$\underline{n = \varepsilon_0 + \varepsilon_1 b + \varepsilon_2 b^2 + \dots + \varepsilon_k b^k = \sum_{i=0}^k \varepsilon_i b^i}$$

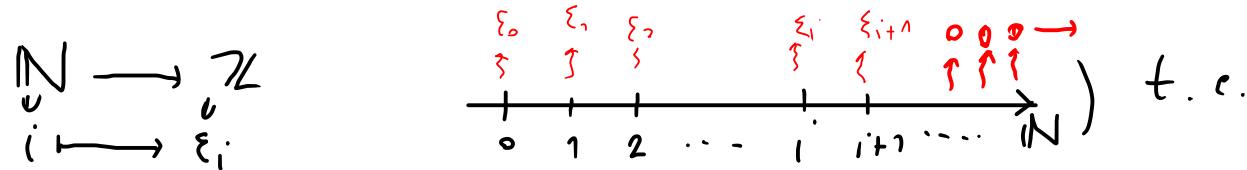
dove $I_b := \emptyset$ se $b=0$ e $I_b := \{0, 1, \dots, b-1\}$ se $b \geq 1$.

OSSERVAZIONE 8.2 (1) Se $b=0$, allora $I_b = \emptyset$. Dunque nessun numero naturale n è rappresentabile in base $b=0$.

(2) Se $b=1$, allora $I_b = I_1 = \{0\}$. Dunque solo $n=0$ è rappresentabile in base $b=1$ (oggi $\varepsilon_i = 0$).]

OSSERVAZIONE 8.3 Sia $b \in \mathbb{N}$ con $b \geq 2$. Osserviamo che un numero naturale $n \in \mathbb{N}$

è rappresentabile in base b se esiste una successione $\{\varepsilon_i\}_{i \in \mathbb{N}}$ di numeri naturali (ovvero



(1) $\{\varepsilon_i\}_{i \in \mathbb{N}}$ è definitivamente nulla (ovvero $\exists K \in \mathbb{N}$ t.c. $\varepsilon_i = 0 \quad \forall i > K$)

(2) $\varepsilon_i \in I_b = \{0, 1, \dots, b-1\} \quad \forall i \in \mathbb{N}$.

$$(3) n = \sum_{i=0}^{\infty} \underbrace{\varepsilon_i b^i}_{\text{se } i > K, \varepsilon_i b^i = 0} = \sum_{i \in \mathbb{N}} \varepsilon_i b^i.$$

OSSERVAZIONE 8.3' Con le notazioni dell'Oss. prec. : $n = (\overbrace{\varepsilon_k \varepsilon_{k-1} \varepsilon_{k-2} \dots \varepsilon_1 \varepsilon_0}^{\leftarrow} \varepsilon_0)_{10}$

- $n = (324)_{10} = 4 \cdot 10^0 + 2 \cdot 10^1 + 3 \cdot 10^2$.

TEOREMA 8.4 (RAPPRESENTAZIONE DI NUMERI NATURALI IN BASE ARBITRARIA ≥ 2)

Sia $b \in \mathbb{N}$ t.c. $b \geq 2$. Allora ogni $n \in \mathbb{N}$ è rappresentabile in modo unico in base b . Ovvero comunque fissato un numero naturale $n \in \mathbb{N}$, esiste una successione $\{\xi_i\}_{i \in \mathbb{N}}$ che ha le prop. viste nell'oss. 8.3. Inoltre se esiste una succ. $\{\xi'_i\}_{i \in \mathbb{N}}$ con le stesse prop. allora $\xi_i = \xi'_i \quad \forall i \in \mathbb{N}$.

DIR. (\exists) Procediamo per induz. su $n \in \mathbb{N}$ (di 2^a forma).

(BASICO INDUT.) $n=0$ È suff. poiché $\xi_i := 0 \quad \forall i \in \mathbb{N}$. OSS. che: $\{\xi_i\}_{i \in \mathbb{N}}$ è sempre nulla (e quindi odef. nulla); $\xi_i = 0 \in I_b = \{0, 1, \dots, b-1\} \quad \forall i \in \mathbb{N}$; $n=0 = \sum_{i=0}^{\infty} \underbrace{\xi_i \cdot b^i}_0$.

(PASSO INDUTTIVO) $n > 0$, $\forall k < n \Rightarrow n$ Sia $n > 0$. Supponiamo che ogni $k \in \mathbb{N}$ con $k < n$ sia rappres. in base b (ip. ind.). Dobbiamo provare che anche n è rappres. in base b .

ESSEGUIAMO LA DIVISIONE EUCLIDEA DI n PER b :

$$\begin{cases} n = qb + r \\ 0 \leq r < b \quad (\text{ovvero } r \in I_b) \end{cases} \quad \text{per qualche (!) } q, r \in \mathbb{N}.$$

Dimostriamo che $q < n$. Se $q = 0$, allora $q = 0 < n$. Se $q > 0$, allora $q < qb \leq qb + r = n$.

Poiché $q < n$, grazie all'ip. ind., q si può rappres. in base b , ovvero $\exists \{\delta_i\}_{i \in I}$ in I_b

(cioè $\delta_i \in I_b$ $\forall i \in \mathbb{N}$) def. nulla e $q = \sum_{i=0}^{\infty} \delta_i \cdot b^i$. Segue che:

$$\begin{aligned} n &= \left(\underbrace{\sum_{i=0}^{\infty} \delta_i \cdot b^i}_q \right) b + r = r + \sum_{i=0}^{\infty} \delta_i \cdot b^{i+1} = r + \sum_{j=1}^{\infty} \delta_{j-1} \cdot b^j = \\ &= rb^0 + \delta_0 b^1 + \delta_1 b^2 + \dots + \delta_{j-1} b^j + \dots = \sum_{i=0}^{\infty} \varepsilon_i \cdot b^i, \end{aligned}$$

dove $\xi_0 := \nu \in I_b$ e $\xi_i := \delta_{i-1} \in I_b \quad \forall i \geq 1$. Dunque, l'elenco soddisfa la tesi prop. dell'os. 8.3.

Segue che il passo induz. è stato fatto. Generalized princ. di induz. di 2^a forma eg. $m \in \mathbb{N}$ è
rapp. in base b.

(!) Procediamo per induz. su $m \in \mathbb{N}$ (di 2^a forma).

(BASE INDUZ.) $m=0$ Si è già visto una succ. def. nulla in I_b t.c. $0=m=\sum_{i=0}^{\infty} \xi_i b^i$.
 $\xi_i \geq 0$

Poiché ciascun prodotto $\xi_i b^i \geq 0$, segue $\xi_i b^i = 0 \quad \forall i \in \mathbb{N}$, ovvero $\xi_i = 0 \quad \forall i \in \mathbb{N}$.

Dunque ogni succ. dell'elenco con la tesi prop. dell'os. 8.3 (con $m=0$) è nulla (e quindi unica).

(PASSO INDUTTIVO) $n > 0$, $\forall k < n \Rightarrow m$ Sia $n > 0$. Assumiamo che ogni $K \in \mathbb{N}$ con $K < n$

ammette una sola rappres. in base (i.p. ind.). Dobbiamo provare che ciò è vero anche per n .

Siano $\{\varepsilon_i\}_{i \in \mathbb{Z}}$ e $\{\varepsilon'_i\}_{i \in \mathbb{N}}$ due succ. in \mathbb{I}_b def. nulle tir.

$$n = \sum_{i=0}^{\infty} \varepsilon_i b^i = \sum_{i=0}^{\infty} \varepsilon'_i b'^i.$$

$$\varepsilon_0 + \varepsilon_1 b' + \varepsilon_2 b'^2 + \dots$$

Vale:

$$\underline{n} = \sum_{i=0}^{\infty} \varepsilon_i b^i = \varepsilon_0 + \left(\sum_{i=1}^{\infty} \varepsilon_i b^{i-1} \right) b = \underline{\left(\sum_{i=1}^{\infty} \varepsilon_i b^{i-1} \right) b + \varepsilon_0},$$

$$\underline{n} = \sum_{i=0}^{\infty} \varepsilon'_i b'^i = \varepsilon'_0 + \left(\sum_{i=1}^{\infty} \varepsilon'_i b'^{i-1} \right) b = \underline{\left(\sum_{i=1}^{\infty} \varepsilon'_i b'^{i-1} \right) b + \varepsilon'_0},$$

dove $0 \leq \varepsilon_0 < b$ e $0 \leq \varepsilon'_0 < b$. Dunque queste uguali sono due divisioni di n per b .

Per unicità della divisione euclidea, segue che $q := \sum_{i=1}^{\infty} \varepsilon_i b^{i-1} = \sum_{i=1}^{\infty} \varepsilon'_i b'^{i-1}$ e $\varepsilon_0 = \varepsilon'_0$.

Ponendo $j := i-1$ e $q = \sum_{j=0}^{\infty} \varepsilon_{j+1} b^j = \sum_{j=0}^{\infty} \varepsilon'_{j+1} b'^j$, per ip. ind. $\varepsilon_{j+1} = \varepsilon'_{j+1} \quad \forall j \in \mathbb{N}$, ovvero

ovvero $\xi_i = \xi'_i \quad \forall i \geq 1$. In conclusione $\xi_i = \xi'_i \quad \forall i \in \mathbb{N}$. Il passo induttivo è stato fatto.

Dunque, grazie al princ. di induz. di 2^a forma, ogni $n \in \mathbb{N}$ ammette una svolta rappres. in base 6. \square

NOTA Suggerisco di leggere OSS. 8.5 (che però non sarà richiesto).

Pag. 23-24, "Il coeff. binomiale" non verrà fatto.]

DIVISIBILITÀ E SUE PRIME PROPRIETÀ (p. 24)

DEF. 9.1 Siano $m, n \in \mathbb{Z}^*$. Diciamo che n è un DIVISORE di m , oppure che m è un
MULTIPLÙ di n , se $\exists k \in \mathbb{Z}$ t.c. $m = kn$. In questo caso, scriveremo $n|m$ che
leggeremo " n divide m ". Scriveremo $n \nmid m$ se n non divide m .]

ESEMPIO 9.2.

(1) $\forall n \in \mathbb{Z}, \quad n|0$ in quanti $n \cdot 0 = 0$.

(2) $\forall n \in \mathbb{Z} \setminus \{0\}, \quad \underset{\substack{\downarrow \\ K \neq 0}}{0 \nmid n}$ in quanti $0 \cdot k = 0 \neq n \quad \forall k \in \mathbb{Z}$.

(3) $\forall n \in \mathbb{Z}, \quad \underset{\substack{\downarrow \\ 0 \mid m}}{\pm 1 \mid m} \quad (\pm 1 \mid m \vee -1 \mid m) \quad \text{e} \quad \underset{\substack{\downarrow \\ \pm 1 \mid m}}{\pm m \mid m}.$

Prop. 9.3 Siano $m, m_1, q \in \mathbb{Z}$. Valgono le seguenti affermazioni:

(1) Se $n|m$ e $n|m_1$, allora $n|m_1$.

(2) Se $n|m$ e $m|m_1$, allora $n=m_1$ oppure $m=\underline{-m_1}$.

DIM. (1) $\exists k, h \in \mathbb{Z}$ t.c. $\underset{\substack{\swarrow \\ k \\ m}}{k \cdot n = m} \quad (\pm 1 \mid m) \quad \text{e} \quad \underset{\substack{\swarrow \\ h \\ m}}{h \cdot m = q} \quad (m \mid q) \Rightarrow q = h \cdot m = h(k \cdot n) = (hk)m \Rightarrow n \mid q.$

(2) Supp. che $n|m$ e $m|n$, ovvero $\exists k, h \in \mathbb{Z}$ t.c. $m = kn$ e $n = hm$. Vale:

$$\underline{n} = \underline{kn} = \underline{k(hm)} = \underline{(kh)m} \Rightarrow \underline{n} - \underline{khm} = \underline{0}$$

\Downarrow
 $m(1 - kh)$

$$\Rightarrow m(1 - kh) = 0 \xrightarrow{m \neq 0} \underline{n} = \underline{h \cdot 0} = \underline{0} = \underline{m}$$

$\Downarrow 1 - kh = 0 \Leftrightarrow kh = 1 \xrightarrow{h=1=k} n = m$
 $\Downarrow h = -1 = k \Rightarrow n = -m.$

DEF. 9.5 (9.7) Siano $n, m \in \mathbb{Z}$ non entrambi nulli. Si dice che $d \in \mathbb{N}$ è un massimo

divisore tra n e m se $d > 0$ e valgono le seguenti due prop.:

(1) $d|n$ e $d|m$.

(2) Se $c \in \mathbb{Z}$ t.c. $c|n$ e $c|m$, allora $c|d$.

Prop. 9.6 (aggiornata) Siano $n, m \in \mathbb{Z}$ non entrambi nulli e siano $d, d' \in \mathbb{N}$ due massimi divisori di n e m ; ovvero $d > 0, d' > 0$ e valgono 1) e 2) sia per d che per d' . Allora $d = d'$.

DIM. $\left. \begin{array}{l} (1) \text{ per } d, (2) \text{ per } d' (c := d) \Rightarrow d \mid d' \\ (1) \text{ per } d', (2) \text{ per } d (c := d') \Rightarrow d' \mid d \end{array} \right\} \xrightarrow{\text{Prop. 2.3 (2)}} d = d'$ oppure $d = -d'$
 in quanto $d > 0$ e $d' > 0$.

$$\Rightarrow d = d'. \quad \square$$

TASSO 8.5 Dati $n, m \in \mathbb{Z}$ non entrambi nulli, esiste ed è unico il massimo comune divisore $\text{m.c.d. } n \text{ e } m$, che verrà indicato (n, m) .

DIM. Dobbiamo provare solo l'esistenza (vedi la prop. prec. per l'unicità).

Definizione $S := \{ s \in \mathbb{N} \mid s > 0 \text{ e } \exists x, y \in \mathbb{Z}, s = xn + ym \}$

$\exists d \in S : S \neq \emptyset, d := \min(S) \rightarrow$ COMPLETARE LA POSSIBILE VOLTA. \square