

Combinamenti di Base

#3.1

Definizione e proprietà dell'operazione modulo n

Notazioni di interesse pratico

- Base 10 : quella che usiamo normalmente
- Base 2 : simboli 0,1 - Prendiamo ϕ_b oppure $()_2$
 $\phi_{b1\phi1\phi}$ per esempio $\bar{=}$ 10 in decimale
- Base 8 : simboli cifre fino al 7
100 in decimale $\bar{=}$ $(144)_8$
- Base 16 : oltre le 10 cifre arabe si aggiungono le prime 5 lettere
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F
Prendiamo ϕ_x
 $0_x 10 \bar{=}$ 16

Combinamento di base Metodo POLINOMIALE

- Deriva dalla definizione di notazione posizionale
- Comodo se si dispone degli operatori algebrici (+, *) nella notazione di ARRIVO

$$a = X_{m-1} B^{m-1} + \dots + X_1 B + X_0$$

si esprimono tutti gli X_i nella nuova base
 si valutano tutte le potenze di B nella nuova base
 si calcola il polinomio

- Una alternativa per il calcolo del polinomio, che evita di eseguire il calcolo delle potenze

$$\underbrace{\left(\dots \left(\left(X_{m-1} B + X_{m-2} \right) B + X_{m-3} \right) B \dots + X_1 \right) B + X_0}_{\text{valore iniziale} \nearrow}$$

- in pratica si parte dalle cifre più significative
- a ogni passo si MOLTIPLICA per B e si somma la cifra di peso inferiore, fino a X_0

$$0_x \text{ FAC342} = 16433986 \quad \left(\left(\left((15 \cdot 16 + 10)_{16} + 12 \right)_{16} + 3 \right)_{16} + 4 \right)_{16} + 2$$

- Il caso binario

Avendo solo 2 casi (somma o non somma il peso), conviene conoscere le potenze del 2 (almeno fino a 2^{12})

| | | | | | | | | | | | | | |
|-------|---|---|---|---|----|----|----|-----|-----|-----|------|------|------|
| i | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 2^i | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4096 |

- Per stimare l'ordine di grandezza di un numero binario, si può osservare che

$$2^{10} \approx 10^3 \quad (1\text{Ki} \text{ un kilo "informatico"})$$

$$2^{20} \approx 10^6 \quad (1\text{Mi} \text{ un Mega})$$

$$2^{30} \approx 10^9 \quad (1\text{Gi} \text{ un Giga})$$

$$2^{40} \approx 10^{12} \quad (1\text{Ti} \text{ un Tera})$$

L'operazione MODULO n - Definizione

- Naturalmente, se si è disposti a usare operatori algebrici in altre basi, il metodo polinomiale può essere usato anche per conversioni con $B \neq 10$.

- Altrimenti possiamo introdurre un nuovo approccio partiamo in \mathbb{N} .

Dati due numeri "a" e "b" (dividendo e divisore), possiamo dimostrare che esiste una unica coppia "q" e "r" tale che, ($b \neq 0$)

$$a = bq + r \quad \text{con } 0 \leq r < b$$

q : quoziente della DIVISIONE INTERA $a : b$

r : resto della divisione intera o $|a|_b$ (a modulo b)

- Come spunto della dimostrazione, osservare che $b \cdot i$ va da \emptyset a un valore grande a piacere ($b \neq 0$) quindi ci sarà un valore di i per cui $b \cdot i \leq a$ e $b \cdot (i+1) > a$. Quel valore è q.

$$r = a - bq \quad \text{poiché } bq \leq a \Rightarrow r \geq 0$$

$$\text{poiché } bq + b > a; \quad bq > a - b \Rightarrow r < a - bq + b$$

Proprietà $| \cdot |_m$

#3.3

• Dalle definizioni derivano utili proprietà

$$|a+b|_m = | |a|_m + |b|_m |_m$$

(1)

$$\left. \begin{aligned} a &= k_a m + |a|_m & b &= k_b m + |b|_m \end{aligned} \right\} \text{dalle definizioni}$$

$$|a \cdot b|_m = | |a|_m \cdot |b|_m |_m$$

(2)

$$|a^k|_m = | |a|_m^k |_m \quad \text{deriva direttamente dal precedente}$$

$$| |a|_m |_m = |a|_m$$

$$|m^x|_m = 0 \quad \forall x \geq 1$$

• Osservare nel caso (1) e (2) che il calcolo del membro DX dell'uguaglianza è più facile (ha numeri più piccoli) del calcolo del membro SX.

Esempio: calcolo del MODULO 9 di un numero scritto in notazione decimale

$$x = 10^{m-1} x_{m-1} + 10^{m-2} x_{m-2} \dots 100 x_2 + 10 x_1 + x_0$$

$$|x|_9 = | |10^{m-1} x_{m-1}|_9 + \dots |10 x_1|_9 + |x_0|_9 |_9$$

ma tutte le potenze di 10 (e potenze da 10) modulo 9 fanno 1 quindi

$$|x|_9 = |x_{m-1}|_9 + \dots + |x_1|_9 + |x_0|_9|_9$$

che è un calcolo molto semplice e può essere usato per verificare la corretta esecuzione di operazioni

$$\begin{array}{r} 194 \times \\ 249 \text{ --- } \times 5 \\ \hline 48306 \text{ --- } \end{array} \quad \begin{array}{r} 5 \\ 6 \times 5 \\ 3 \\ 3 \end{array} \quad |6 \times 5|_9$$

Prova del "9"

- Se vogliamo usare per la conversione l'algebra nella base di partenza (quella decimale tipicamente) possiamo usare un metodo ITERATIVO

$$x_0 = B^{m-1} X_{m-1} + \dots + B X_1 + X_0$$

$$\begin{cases} X_0 = |x_0|_B \\ x_1 = x_0 : B \text{ (divisione intera)} \end{cases}$$

$$\begin{cases} X_1 = |x_1|_B \\ x_2 = x_1 : B \end{cases}$$

e così via, fino a quando $x_i = \emptyset$

- Esempio da base 10 a base 2

| | | | |
|------|-----|----------|-------|
| 1824 | mod | 0 | x_0 |
| 912 | 0 | x_1 | |
| 456 | 0 | x_2 | |
| 228 | 0 | x_3 | |
| 114 | 0 | x_4 | |
| 57 | 1 | x_5 | |
| 28 | 0 | x_6 | |
| 14 | 0 | x_7 | |
| 7 | 1 | x_8 | |
| 3 | 1 | x_9 | |
| 1 | 1 | x_{10} | |
| 0 | | | |

$$1824 = 0b11100100000$$

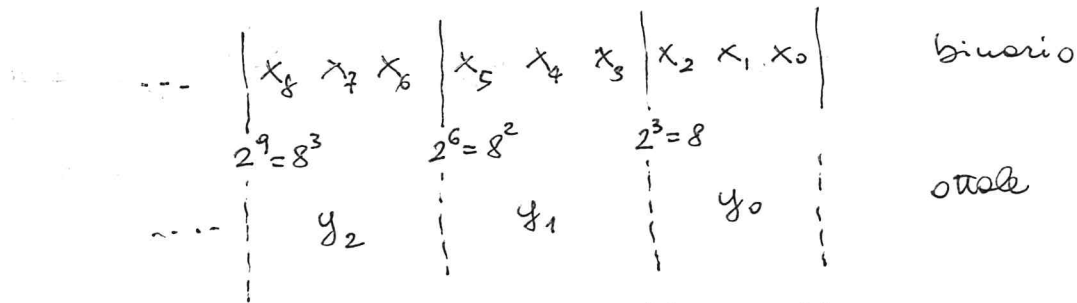
- Da base 10 a base 3

| | | |
|----|---------------------|---|
| 77 | mod (sommare cifre) | 2 |
| 25 | 1 | |
| 8 | 2 | |
| 2 | 2 | |
| 0 | | |

$$77 = (2212)_3 = 2 + 3 + 18 + 54$$

Passaggio tra basi potenze di 2 e binario

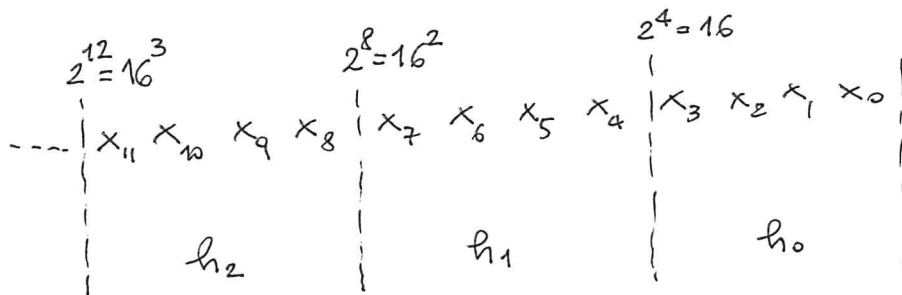
- Particolarmente interessante il passaggio tra base 2 \Rightarrow base 8 e tra base 2 \Rightarrow base 16. Caso ottale: RAGGRUPPO A TERNE



relazione tra cifre binarie e cifre ottali

$$y_i = x_{3i} + 2x_{3i+1} + 4x_{3i+2}$$

- Caso esadecimale: RAGGRUPPO A QUATERNE



Esempi

$$0x \text{ FAC3} = 0b \overset{F}{1111} \overset{A}{1010} \overset{C}{1100} \overset{3}{0011}$$

$$0b \overset{5}{1011} \overset{D}{1011} \overset{C}{1100} = 0x \text{ 5DC}$$