Cambiamenti di Base
Definizione e proprietà dell'operazione modulo n

Notazioni di interesse pratico

- Base 10 : quella che usiamo normalmente
- Base 2 : simboli 0, 1 – Premettiamo 0b oppure $(\ )_2$
  0b1010 per esempio è 10 in decimale
- Base 8 : simboli cifre fino al 7
  100 in decimale è $(144)_8$
- 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
  Premettiamo 0x
  0x10 è 16

Cambiamento di base Metodo POLINOMIALE

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

$$x = X_{n-1} B^{n-1} + \dots X_1 B + X_0$$

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

$$(\dots(((X_{n-1}B + X_{n-2})B + X_{n-3})B \dots + X_1)B + X_0$$

valore iniziale → X_{n-1}

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

0xFAC342 = 16433986 $\quad ((((15 \cdot 16+10)16+12)16+3)\cdot 16+4)16+2$

- Il caso binario
  Avendo solo 2 casi (sommo o non sommo 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

  $2^{10} \simeq 10^3$ (1Ki un kilo "informatico")
  $2^{20} \simeq 10^6$ (1Mi un Mega)
  $2^{30} \simeq 10^9$ (1Gi un Giga)
  $2^{40} \simeq 10^{12}$ (1Ti 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. Restiamo in $\mathbb{N}$.
  Dati due numeri "a" e "b" (dividendo e divisore), possiamo dimostrare che esiste una unica coppia "q" e "r" tale che, $(b \neq 0)$

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

  q : quoziente della DIVISIONE INTERA $a:b$
  r : resto della divisione intera o $|a|_b$ (a modulo b)

- Come spunto della dimostrazione, osservo 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 $bi \leq a$ e $b(i+1) > a$.
  Quel valore è q.

  $r = a - bq$ poiché $bq \leq a \Rightarrow r \geq \emptyset$
  poiché $bq + b > a$; $bq > a - b \Rightarrow r < \cancel{a} - \cancel{a} + b$

Proprietà $|\cdot|_n$

- Dalla definizione derivano utili proprietà

$$|a+b|_n = \big|\, |a|_n + |b|_n \big|_n \qquad (1)$$

$a = k_a n + |a|_n \qquad b = k_b n + |b|_n$

dalla definizione

$$|a \cdot b|_n = \big|\, |a|_n \cdot |b|_n \big|_n \qquad (2)$$

$$|a^k|_n = \big|\, |a|_n^k \big|_n$$ deriva direttamente dal precedente

$$\big|\, |a|_n \big|_n = |a|_n$$

$$|n^x|_n = \varnothing \qquad \forall\, x \geq 1$$

- 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

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

$$|x|_9 = \big|\, |10^{n-1} x_{n-1}|_9 + \ldots \quad |10 x_1|_9 + |x_0|_9 \big|_9$$

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

$$|x|_9 = \big|\, |x_{n-1}|_9 + \ldots + |x_1|_9 + |x_0|_9 \big|_9$$

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

Prova del "9"

```
  194 x        5
  249       6  X  3     |6x5|9
-----          3
48306
```

Cambio BASE con divisione intera e modulo B

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

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

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

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

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

- Esempio da base 10 a base 2

	mod	
1824	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 = Øb111ØØ1ØØØØØ

Da base 10 a base 3

	mod (sommare cifre)
77	2
25	1
8	2
2	2
Ø	

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

Passaggio tra basi potenze di 2 e binario

– Particolarmente interessante il passaggio tra base 2 ⇄ base 8 e tra base 2 ⇄ base 16. Caso ottale: RAGGRUPPO A TERNE

...	x_8 x_7 x_6	x_5 x_4 x_3	x_2 x_1 x_0	binario
	$2^9=8^3$	$2^6=8^2$	$2^3=8$	
...	y_2	y_1	y_0	ottale

relazione tra cifre binarie e cifre ottali

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

- Caso esadecimale: RAGGRUPPO A QUATERNE

	$2^{12}=16^3$	$2^8=16^2$	$2^4=16$
...	x_{11} x_{10} x_9 x_8	x_7 x_6 x_5 x_4	x_3 x_2 x_1 x_0
	h_2	h_1	h_0

Esempi

		F	A	C	3
0xFAC3	=	0b 1111	1010	1100	0011

0b 101	1101	1100	=	0x5DC
5	D	C		