

Fondamenti di Informatica  
per la Sicurezza  
a.a. 2006/07

## Concetto di numero

**Stefano Ferrari**



UNIVERSITÀ DEGLI STUDI DI MILANO  
DIPARTIMENTO DI TECNOLOGIE DELL'INFORMAZIONE

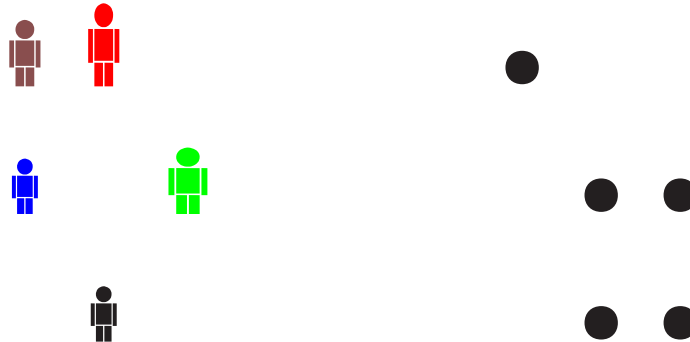
### Aforisma

---

Aritmetica è contare fino a venti  
senza togliersi le scarpe  
[Topolino]

## Numeri

Un numero è un ente astratto usato per indicare proprietà *quantitative* delle grandezze.



## Contare

Per contare, non è necessario conoscere i numeri.  
Basta ricorrere a delle relazioni:

- tra grandezze discrete:
  - sassolini e pecore;
  - dita della mano e figli.
- tra grandezze continue:
  - tempo trascorso e candela che brucia;
  - tempo trascorso e spazio percorso dall'ombra.

## Astrazione

---

Le esigenze pratiche possono portare a scoprire concetti più evoluti.

Alcuni esempi:

- confronto tra elementi numerici;
- proprietà delle operazioni;
- assegnazione di nomi a numeri particolari;
- concetto di ordine di grandezza.

## Rappresentazione dei numeri

---

L'elaborazione (o la trasmissione) dei numeri richiede la loro rappresentazione su di un supporto fisico.

Serve quindi:

- mezzo fisico (modificabile, ma stabile);
- codifica.

## Sistema di numerazione

---

Codifica *arbitraria* per rappresentare un *insieme infinito* di oggetti utilizzando un *insieme finito* di simboli.

## Numerale

---

Al concetto astratto di *numero* si affianca la sua rappresentazione simbolica: il **numera**le.

Interpretazione del numerale:

- un numerale ha significato solo all'interno di un sistema di numerazione.

## Sistemi di numerazione

I sistemi di numerazione si dividono principalmente in:

- additivi;
- posizionali.

## Sistemi di numerazione additivi (1)

Sistema di numerazione romano:

- in uso nell'antica Roma;
- simboli letterali: I, V, X, L, C, D e M (uno, cinque, dieci, cinquanta, cento, cinquecento e mille);
- i simboli affiancati in ordine decrescente indicano il numero pari alla loro somma;
- se un simbolo precede un simbolo di valore superiore, deve essere sottratto.

## Sistemi di numerazione additivi (2)

Sistema di numerazione romano:

- esempio:

MCMLXII

$$1000 + (1000 - 100) + 50 + 10 + 1 + 1$$

1962

## Sistemi di numerazione posizionali

Notazione decimale:

- inventata in India, perfezionata dagli arabi e poi introdotta in Europa da Fibonacci;
- basata su dieci cifre;
- il significato dipende dalla loro posizione.
- Esempio:

$$1203 = 1 \cdot 10^3 + 2 \cdot 10^2 + 0 \cdot 10^1 + 3 \cdot 10^0$$

## Numeri e rappresentazione

Il concetto di “numero” è *indipendente* dalla sua rappresentazione.

Esempio:

+ + + o + o + o o o + o + o o o + o + o

In questo caso, i simboli “+” sono posizionati in corrispondenza di un numero primo.

La scelta della rappresentazione dipende dall’utilizzo che si vuol fare dei numeri rappresentati.

## Scelta della notazione posizionale

Se si devono fare calcoli, la notazione posizionale offre alcuni indubbi vantaggi.

Proprietà della notazione posizionale:

- **somma**: viene operata agendo “localmente” (unità con unità, decine con decine e così via);
- **traslazione (shift)**: moltiplicare o dividere per 10 trasla le cifre di una posizione;
- **compattezza**: la rappresentazione richiede un numero di cifre logaritmico.

## Notazione posizionale (1)

Formalizzazione:

$$(a_n \dots a_1 a_0)_b \equiv \sum_{i=0}^n a_i \cdot b^i, \quad b \geq 2, \quad a_i \in \{0, \dots, b-1\}$$

- dato un numero intero maggiore o uguale a 2,  $b$ , detto *base*,
- la sequenza  $a_n \dots a_1 a_0$ ,
- composta da  $n + 1$  simboli scelti dall'insieme  $\{0, \dots, b-1\}$ ,
- viene interpretata come  $a_n \cdot b^n + \dots + a_1 \cdot b^1 + a_0 \cdot b^0$ .

## Notazione posizionale (2)

Basi notevoli:

- decimale,  $b = 10 \quad a_i \in \{0, \dots, 9\}$ ;
- binaria,  $b = 2 \quad a_i \in \{0, 1\}$ ;
- ottale,  $b = 8 \quad a_i \in \{0, \dots, 7\}$ ;
- esadecimale,  $b = 16 \quad a_i \in \{0, \dots, 9, A, \dots, F\}$ .

Esempi:

- $(34)_{10} = 3 \cdot 10 + 4 \cdot 1 = 34$
- $(34)_8 = 3 \cdot 8 + 4 \cdot 1 = 28$
- $(34)_{16} = 3 \cdot 16 + 4 \cdot 1 = 52$



## Tuttavia ...

In alcuni campi, è più comodo usare una base diversa da quella decimale.

Infatti:

- le uova si vendono a dozzine;
- le ore sono composte da 60 minuti;
- un giorno dura 24 ore.

12 è divisibile per 2, 3, 4 e 6!

## Numeri frazionari

Ogni numero intero è rappresentabile utilizzando una qualsiasi base, ma lo stesso non vale per i numeri frazionari:

in base 10  $\frac{1}{3} \equiv (0.\bar{3})_{10}$

in base 3  $\frac{1}{3} \equiv (0.1)_3$

I numeri frazionari si possono rappresentare come:

$$(a_n \dots a_2 a_1 a_0 . a_{-1} \dots a_{-m})_b \equiv \sum_{i=-m}^n a_i \cdot b^i, \quad b \geq 2$$

## Cambio di base (1)

Come si scrive in base 12 il numero rappresentato dal numerale  $(32)_4$ ?

NB: Cambia solo la ***rappresentazione*** del numero!

Per rispondere alla domanda serve una piccola digressione: la divisione.

## Divisione

Dati due numeri naturali  $a, b$  ( $b > 0$ ), la divisione permette di determinare due numeri  $q$  ed  $r$  tali che

$$a = b \cdot q + r, \quad 0 \leq r < b$$

dove:

- $a$  è il *dividendo*;
- $b$  è il *divisore*;
- $q$  è il *quoziente* (o *quoto*);
- $r$  è il *resto*.

## Cambio di base (2)

L'algoritmo per il cambio di base fa uso degli operatori di divisione intera (***div***) e di resto (***mod***):

***div*** è la parte intera della divisione tra due numeri interi (*quoziente*):

es:  $13 \text{ div } 5 = 2$

***mod*** è il *resto* della divisione tra due numeri interi:

es:  $13 \text{ mod } 5 = 3$

Infatti:

$$13 = 5 \cdot 2 + 3$$

## Cambio di base (3)

Algoritmo per trovare il numerale del numero  $n$ , in una data base,  $b$ :

1. Calcolare il quoziente,  $q$ , ed il resto,  $r$ , della divisione di  $n$  per  $b$ :  
 $q = n \text{ div } b$   
 $r = n \text{ mod } b$
2. Il resto,  $r$ , è l'ultima cifra del numerale che esprime  $n$  in base  $b$ .
3. Se il quoziente,  $q$ , è diverso da zero, le rimanenti cifre si ottengono trasformando il quoziente, sostituendo nei passi precedenti  $q$  ad  $n$ .
4. Se il quoziente è zero, la conversione è terminata.

## Cambio di base (4)

Esempio:  $(133)_{10} \rightarrow (x)_5$

quoziente	resto	
133		$133 = 26 \cdot 5 + 3$
26	3	$26 = 5 \cdot 5 + 1$
5	1	$5 = 1 \cdot 5 + 0$
1	0	$1 = 0 \cdot 5 + 1$
0	1	

$$(133)_{10} = (1013)_5$$

## Cambio di base (5)

Spiegazione:

$$\begin{aligned}
 133 &= 26 \cdot 5 + \mathbf{3} = \\
 &= (5 \cdot 5 + \mathbf{1}) \cdot 5 + \mathbf{3} = \\
 &= ((1 \cdot 5 + \mathbf{0}) \cdot 5 + \mathbf{1}) \cdot 5 + \mathbf{3} = \\
 &= (((0 \cdot 5 + \mathbf{1}) \cdot 5 + \mathbf{0}) \cdot 5 + \mathbf{1}) \cdot 5 + \mathbf{3} = \\
 &= ((\mathbf{1} \cdot 5 + \mathbf{0}) \cdot 5 + \mathbf{1}) \cdot 5 + \mathbf{3} = \\
 &= (\mathbf{1} \cdot 5^2 + \mathbf{0} \cdot 5 + \mathbf{1}) \cdot 5 + \mathbf{3} = \\
 &= \mathbf{1} \cdot 5^3 + \mathbf{0} \cdot 5^2 + \mathbf{1} \cdot 5 + \mathbf{3} = \\
 &= \mathbf{1} \cdot 5^3 + \mathbf{0} \cdot 5^2 + \mathbf{1} \cdot 5 + \mathbf{3} \cdot 5^0
 \end{aligned}$$

$$(133)_{10} = (1013)_5$$

## Numero di cifre (1)

Quante cifre,  $k$ , bisogna usare per rappresentare in base  $b$  il numero  $n$ ?

Ragionando in base 10:

con 1 cifra:  $0 \dots 9$  fino a  $10^1 - 1$

con 2 cifre:  $10 \dots 99$  fino a  $10^2 - 1$

con 3 cifre:  $100 \dots 999$  fino a  $10^3 - 1$

con  $k$  cifre:  $10^{k-1} \dots 10^k - 1$  fino a  $10^k - 1$

$k$  deve essere il più piccolo numero intero tale per cui  $b^k - 1 \geq n$ .

Per comodità:  $b^k \geq n + 1$ .

## Numero di cifre (2)

Applicando il logaritmo in base  $b$  ad entrambi i membri della disequazione precedente:

$$\log_b b^k \geq \log_b (n + 1)$$

$$k \geq \log_b (n + 1)$$

$$k = \lceil \log_b (n + 1) \rceil$$

dove  $\lceil x \rceil$  indica il più piccolo numero intero maggiore o uguale a  $x$ .

## Numero di cifre (3)

Quante cifre sono necessarie per rappresentare 1145 in notazione posizionale in base:

a) 10    b) 2    c) 16?

a) 10:  $\log_{10} 1146 \approx 3.0592 \rightarrow 4$  cifre.

Infatti:  $1145 = (1145)_{10}$ .

b) 2:  $\log_2 1146 \approx 10.162 \rightarrow 11$  cifre.

Infatti:  $1145 = (10001111001)_2$ .

c) 16:  $\log_{16} 1146 \approx 2.5406 \rightarrow 3$  cifre.

Infatti:  $1145 = (479)_{16}$ .

## Da base $n$ a decimale

Come si rappresenta in base 10 il numero  $(412)_5$ ?

Dalla definizione di notazione posizionale:

$$\begin{aligned} (412)_5 &= 4 \cdot 5^2 + 1 \cdot 5^1 + 2 \cdot 5^0 = \\ &= 4 \cdot 25 + 1 \cdot 5 + 2 \cdot 1 = \\ &= 100 + 5 + 2 = \\ &= 107 \end{aligned}$$

$$(412)_5 = (107)_{10}$$

## Da decimale a base $n$

Come si rappresenta in base 3 il numero  $(1079)_{10}$ ?

Algoritmo della divisione:

quoziente	resto
1079	
359	2
119	2
39	2
13	0
4	1
1	1
0	1

$$(1079)_{10} = (1110222)_3$$

## Da base $m$ a base $n$ (1)

Come si rappresenta in base 5 il numero  $(106)_7$ ?

Si potrebbe applicare l'algoritmo di divisione, ma è difficile fare i calcoli se la base non è 10.

Meglio risolvere il problema in due passi:

1. conversione da base 7 a decimale;
2. conversione da decimale a base 5.

## Da base $m$ a base $n$ (2)

Conversione da base 7 a decimale:

$$(106)_7 = 1 \cdot 7^2 + 0 \cdot 7^1 + 6 \cdot 7^0 = 55$$

Conversione da decimale a base 5:

quoziente	resto
55	
11	0
2	1
0	2

Quindi:

$$(106)_7 = (210)_5$$

## Da binario ad ottale

È un caso particolare di conversione da base  $m$  a base  $n$ :  $8 = 2^3$ .

Se  $n = m^k$ , il cambiamento di base si può operare per blocchi.

Esempio:  $(101001)_2 = (???)_8$

$$\begin{aligned}
 (101001)_2 &= \\
 &= 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = \\
 &= (1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0) \cdot 2^3 + (0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0) \cdot 2^0 = \\
 &= (5) \cdot 8^1 + (1) \cdot 8^0 = \\
 &= (51)_8
 \end{aligned}$$

base 2	101	001
base 8	5	1



## Da binario ad esadecimale

È un caso particolare di conversione da base  $m$  a base  $n$ :  $16 = 2^4$ .

Esempio:  $(101001010)_2 = (???)_{16}$

base 2	0001	0100	1010
base 16	1	4	A

$$(101001010)_2 = (14A)_{16}$$

## Da ottale a binario

È un caso particolare di conversione da base  $m$  a base  $n$ :  $8 = 2^3$ .

Se  $m = n^k$ , il cambiamento di base si può operare per blocchi.

Esempio:  $(51)_8 = (???)_2$

$$\begin{aligned}
 &= (51)_8 = (5) \cdot 8^1 + (1) \cdot 8^0 = \\
 &= (1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0) \cdot 2^3 + (0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0) \cdot 2^0 = \\
 &= 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = \\
 &= (101001)_2
 \end{aligned}$$

base 8	5	1
base 2	101	001

## Da esadecimale a binario

È un caso particolare di conversione da base  $m$  a base  $n$ :  $16 = 2^4$ .

Esempio:  $(14A)_{16} = (???)_2$

base 16	1	4	A
base 2	0001	0100	1010

$$(14A)_{16} = (101001010)_2$$