SISTEMI DI NUMERAZIONE

Il nostro è un sistema decimale

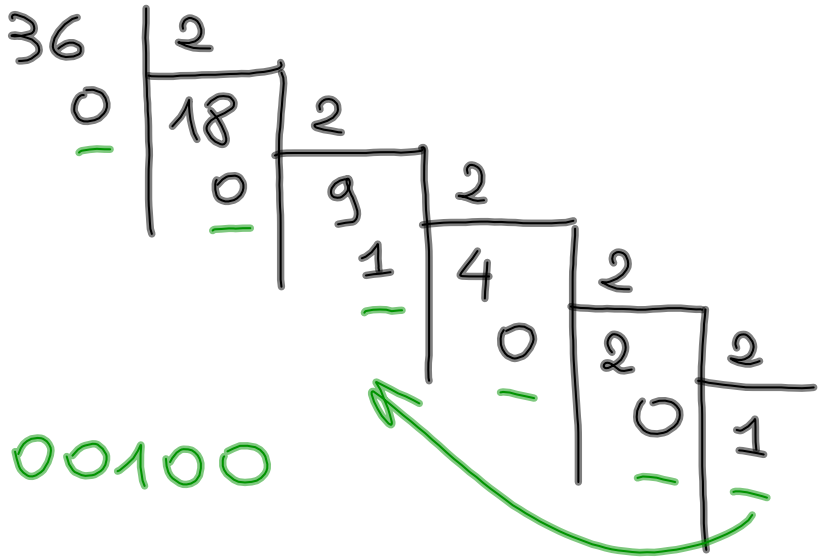
Utilizziamo 10 cifre: 0, 1, 2, ... 9

Il sistema binario o in base 2

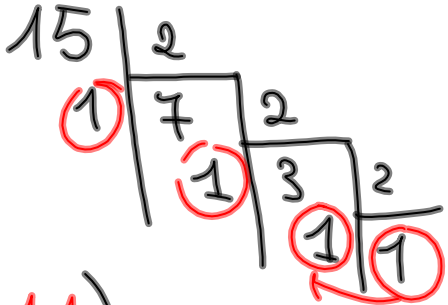
ha 2 cifre: 0, 1.

Era gia' conosciuto dai Cinesi in antichita'. Leibniz nel XVII secolo ebbe per primo l'intuizione di trascrivere ogni frase in successioni di 0 e 1, in modo da creare un linguaggio universale

$(36)_{10} \rightarrow (\quad)_2$



100100



$(15)_{10} = (1111)_2$

Per trasformare un numero dalla base 10 alla base 2 si effettuano le divisioni ripetute per 2, finche' si ottiene 1 come ultimo quoziente.Il numero in base 2 e' dato da questo quoziente, seguito da tutti i resti presi in ordine dall'ultimo al primo, come indicato dalla freccia.

$(10110)_2 \longrightarrow (\quad)_{10}$

$34 = 4 \cdot 10^0 + 3 \cdot 10^1$

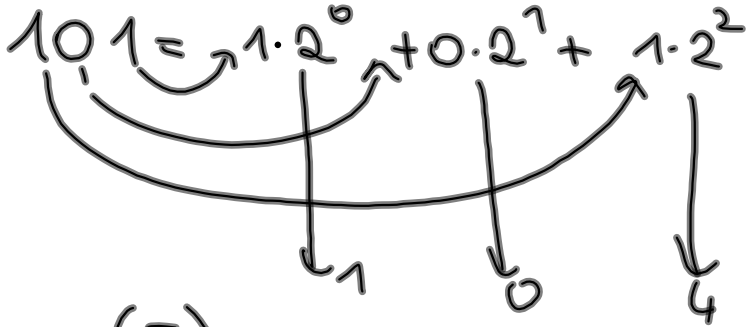
NOTAZIONE POSIZIONALE

$43 = 3 \cdot 10^0 + 4 \cdot 10^1$

X M non è posizionale

La binaria è posizionale

il valore di una cifra cambia a seconda della sua posizione



Anche il sisema decimale e' posizionale. Se scrivo 21 la cifra 2 indica 20 unita', se scrivo 32 la cifra 2 indica 2 unita'.

$(101)_2 \rightarrow (5)_{10}$ $\quad 1+4 = (5)$

$10110 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4$

2 4 16

$= (22)_{10}$

$(1100)_2 = 1 \cdot 2^2 + 1 \cdot 2^3 = (12)_{10}$

Con una base diversa da 2 il procedimento e' lo stesso. Ad esempio, in base 3

$$(2012)_3 = 2\cdot 3^0 + 1\cdot 3^1 + 0\cdot 3^2 + 2\cdot 3^3$$

$$= 2 + 3 + 0 + 54$$

$$= 59$$

$$(2012)_3 = (59)_{10}$$

BASE 5

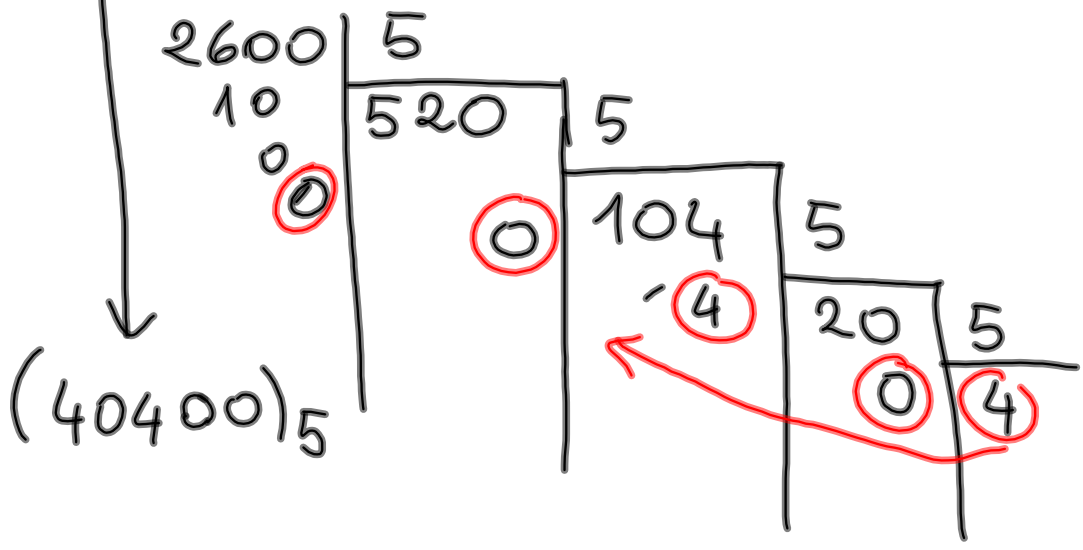
le cifre sono 0, 1, 2, 3, 4

$(4201)_5 \rightarrow 1 \cdot 5^0 + 2 \cdot 5^2 + 4 \cdot 5^3$

$= 1 + 50 + 500$

$= (551)_{10}$

$(2600)_{10}$



$(40400)_5$

La numerazione in base 2 e' importante perche' e' utilizzata nei circuiti elettrici digitali

0 → interruttore spento

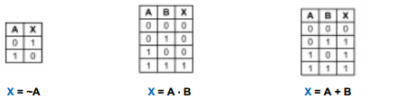
1 → interruttore acceso

oppure verita' di una formula

0 → falso

1 → vero

Tabelle di verità di NOT, AND, OR



http://www.dsi.unive.it/~arcb/AA00-01/SLIDES/bool4.pdf

L'unita' di misura della memoria di un computer e' il byte. Un byte e' composto da 8 bit. Il termine bit deriva dalla contrazione delle parole binary digit. Le informazioni vengono tradotte all'interno dei computer in successioni di 0 e 1.

Ogni carattere della tastiera viene tradotto in una successione di 8 cifre che possono essere 0 o 1. Ad esempio la lettera

a e' rappresentata da 01100001, la lettera b da 01100010

altri esempi in tabella:

codice ASCII

American Standard Code for Information Interchange

Binary Bits	Character	ASCII
01001000	H	72
01100101	e	101
01101100	l	108
01101100	l	108
01101111	o	111
00100000	space	32
01001010	J	74
01101111	o	111
01110011	s	115
01101000	h	104
01110101	u	117
01100001	a	97

Premi il tasto Alt sulla tastiera e il numero del codice ASCII

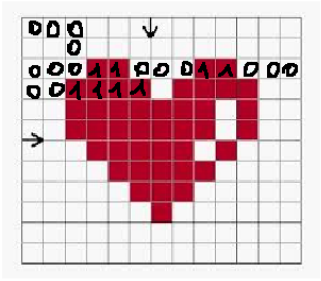
ad esempio con Alt 97 si ottiene la lettera a

Le stesse operazioni possono essere rappresentate con successioni di 0 e 1. Ad esempio la somma con 0000, la moltiplicazione con 0010, ecc.

Anche le immagini possono essere rappresentate in base 2!

In bianco e nero → 0 bianco
1 nero

L'immagine si suddivide in caselle chiamate PIXEL



per le immagini a colori ad ogni pixel viene associata una sequenza di bit

ADDIZIONI IN BASE 2

$0+0=0$

$1+0=1$

$1+1=10$

$$\begin{array}{r} 1011+ \\ 101= \\ \hline 10000 \end{array}$$

$$\begin{array}{r} 101\times \\ 100= \\ \hline 101-- \\ 10100 \end{array}$$

$$\begin{array}{r} 101\times \\ 11= \\ \hline 101 \\ 101- \\ \hline 1111 \end{array}$$

$$\begin{array}{r} 1011- \\ 101= \\ \hline 110 \end{array}$$

$10-1=1$

perché: $(1+1=10)$

$$\begin{array}{r} 100- \\ 11= \\ \hline -1 \end{array}$$

$10-1$

$$\begin{array}{r} 10110- \\ 111= \\ \hline 1111 \end{array}$$

CONTIAMO IN BASE 2

0

1

10

11

100

101

110

111

1000

1001

1010

1011

⋮

OPERAZIONI

$$\begin{array}{r} 100 - \\ 11 = \\ \hline \end{array}$$

$1 - 0 = 1$

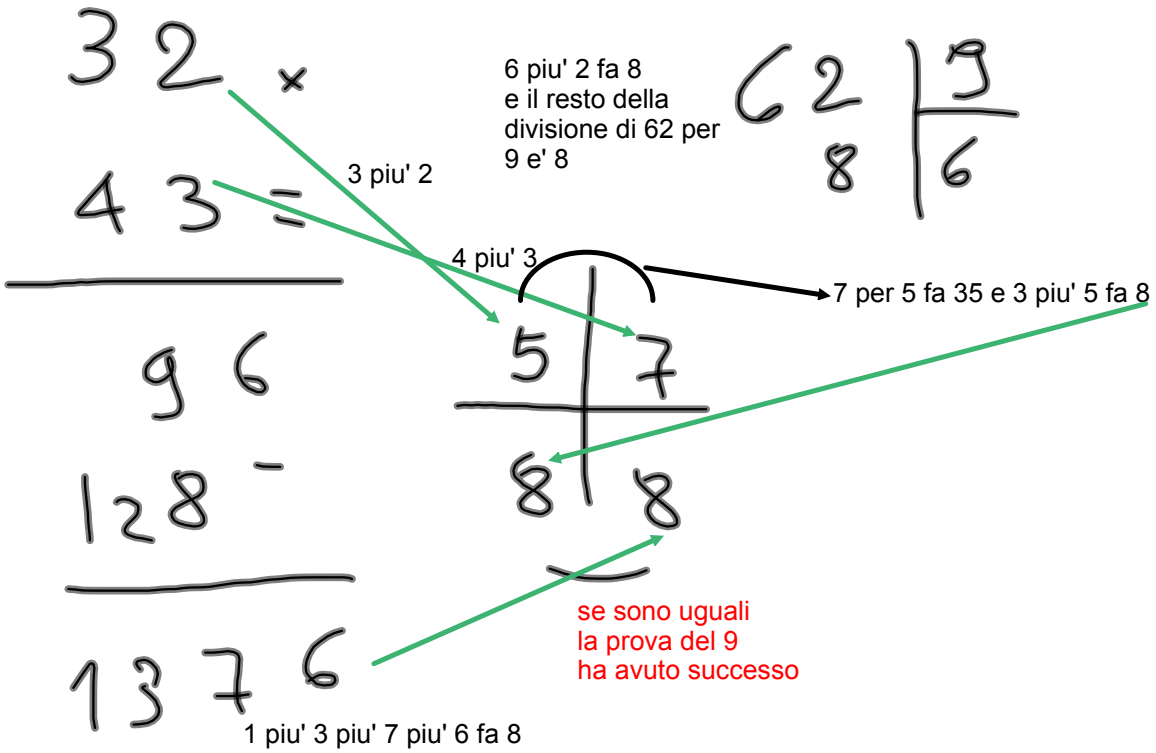
$1 - 1 = 0$

$0 - 1$ IMPOSS.

A MENO che si prende in prestito un "1" dalla cifra precedente

PROVA del NOVE

La somma delle cifre di un numero e' uguale al resto della divisione del numero per nove



La prova del 9 costituisce una condizione necessaria, ma non sufficiente, affinche' l'operazione sia stata eseguita correttamente

quando troviamo la cifra 9 in un numero, possiamo considerarlo come se fosse 0, perche' il resto della divisione di 9 per 9 e' 0.

CLASSI RESTO MODULO 9

$[0] = \{9; 18; 27; \dots\}$

$[1] = \{10; 19; 28; \dots\}$

$[2] = \{11; 20; 29; \dots\}$

$\vdots$

$[8]$

Le classi resto sono classi di equivalenza

Un'interessante applicazione delle classi resto e' nella cifratura dei messaggi

Crittografia ed Aritmetica Modulare
LABORATORIO del III incontro
– con Soluzioni –

PLS - CAM

Padova, 31 ottobre 2014

Esercizio 1.3. *Oggi, martedì 3 aprile, alle ore 21, devo prendere un treno per la Transilvania che mi porterà a destinazione in 57 ore. In che giorno ed a che ora arriverò?*

Svolgimento. Se sommo le 57 ore del viaggio alle ore 21 della partenza, ottengo 78 ore. Eseguendo la divisione intera per 24 ottengo:

$$78 = 24 \cdot 3 + 6$$

il che significa che arriverò 3 giorni dopo, cioè venerdì 6 aprile, alle ore 6. ∎

Quesito 1. Qual è la differenza fra steganografia e crittografia?

Nella steganografia il messaggio non viene alterato, bensì nascosto. Nella crittografia il messaggio viene invece cifrato, cioè se ne rende incomprensibile il significato attraverso una alterazione del messaggio stesso attuata per mezzo di un processo segreto ma reversibile.

Quesito 2. Qual è il metodo utilizzato per attaccare i sistemi crittografici di Cesare e Vigenère?

Principalmente il metodo basato sull'analisi delle frequenze, una volta che sia nota la lingua con la quale è stato scritto il testo originale. Nel caso più complesso di Vigenère appare indispensabile comprendere dapprima quale sia la lunghezza della chiave di cifratura, e questo è possibile attraverso la ricerca delle ripetizioni di sequenze di caratteri, rilevandone la distanza.

Quesito 3. i) Si consideri a^2 con a numero intero. Provare che il resto della divisione per 4 del numero a^2 è 0 oppure 1.

Se a è pari, allora è divisibile per 2, e così a^2 è divisibile per 4, cioè a^2 è congruo a 0 modulo 4. Se, al contrario, a è dispari, allora è della forma $a = b+1$ con b intero pari. Così $a^2 = (b+1)^2 = b^2+2b+1$. Ora b^2+2b è divisibile per 4, ed allora a^2 è congruo a 1 modulo 4.

ii) Usare il punto precedente per trovare i possibili resti della divisione per 4 del numero $a^2 + b^2$.

Se a e b sono entrambi pari, allora per quanto visto nel punto precedente sia a^2 che b^2 sono congrui a 0 modulo 4, e così pure a^2+b^2 è congruo a 0 modulo 4. Se invece uno dei due è pari e l'altro è dispari, allora il quadrato del primo è congruo a 0 modulo 4 mentre il quadrato del secondo è congruo a 1 modulo 4, ed allora a^2+b^2 è congruo a 1 modulo 4. Infine, se a e b sono entrambi dispari, allora sia a^2 che b^2 sono congrui a 1 modulo 4, e così a^2+b^2 è congruo a 2 modulo 4. I resti possibili sono in definitiva 0, 1 e 2.

Quesito 4. Dimostrare che per un numero intero $x \in \mathbb{Z}$ vale

$$\begin{cases} x \equiv 1 \text{ mod. } 2 \\ x \equiv 1 \text{ mod. } 3 \\ x \equiv 1 \text{ mod. } 5 \end{cases}$$

se e solo se

$$x \equiv 1 \text{ mod. } 30.$$