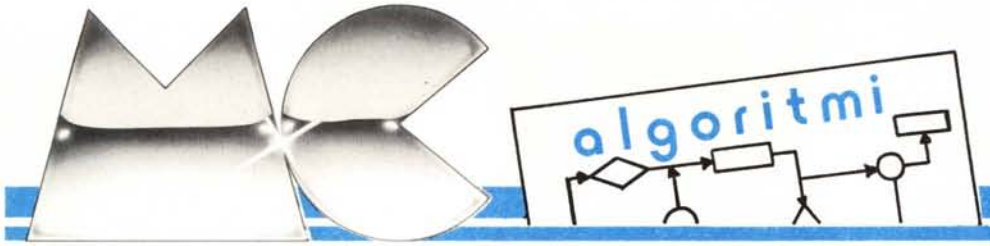


di Raffaello De Masi

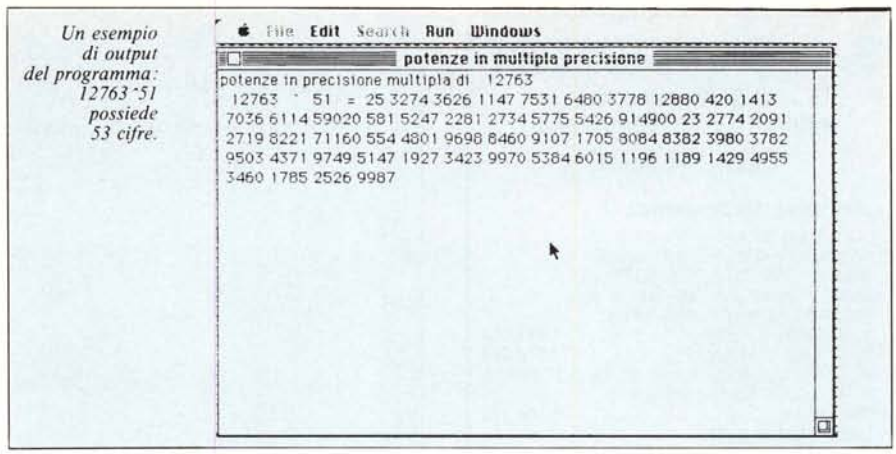
Alcuni tool di base per lo sviluppo di algoritmi più complessi

Quanto diremo in questa puntata ed in alcune prossime, pur se interessante in sé, e destinato a poter essere utilizzato tal quale per scopi particolari di chi legge, è stato preparato in quanto ci permetterà di disporre di mezzi per lo sviluppo di argomenti un po' più complessi. Tanto per intenderci, ricordate la lettera di un lettore, di qualche mese fa, che proponeva un codice di cifrazione di messaggi carbonaro, peraltro di non difficile risoluzione? Parleremo, in una delle prossime puntate, delle tecniche di codifica dei messaggi scritti, e di come sia possibile implementare le stesse in un computer; ovviamente cercheremo di essere semplici, esponendo solo le tecniche di più agevole ed immediata comprensione (esiste, negli U.S.A. una casa editrice che ha in catalogo solo pubblicazioni dedicate alla crittografia dei messaggi, circa una settantina di titoli, prevalentemente materiale militare reso pubblico). Per lo sviluppo di tale argomento, e, in particolare, per l'analisi dei più sofisticati procedimenti di crittografia, come ad esempio quello a trasformazione di matrice od a chiave pubblica, occorre conoscere alcune tecniche particolari, come operazioni su matrici e manipolazione di grandi numeri. Di queste tecniche contiamo qui di dare qualche cenno; probabilmente non saremo esaurienti su tutti gli aspetti di tali pur interessanti argomenti, ma non desideravamo esserlo, visto che testi ben più complessi e completi sono stati scritti, sui temi di cui accenniamo, da autori specializzati, di cui alla fine forniremo una bibliografia.

Uno dei più grossi problemi di un calcolatore è quello di manipolare numeri dotati di numerose cifre. Tanto per intenderci utilizzando un computer (od anche una normale calcolatrice tascabile) è praticamente impossibile conoscere il preciso risultato di operazioni, nel caso più semplice ed ovvio moltiplicazioni, coinvolgenti, come valore finale o come input numeri di lunghezza superiore ad un certo gruppo

```
'                potenze in multipla precisione
'
'            questo programma stampa potenze in multipla precisione
'              fino a raggiungere una lunghezza di cifre prefissate
'
'           il numero di cifre massime è determinato dal valore della x
'                nella riga con label "cifre" , secondo la formula :
'             numero delle cifre = valore di (variabile x+1) * 4
'
'
zero:
  CLS
  WIDTH 60
  PRINT "questo programma stampa potenze di un numero fino a 36 cifre decimali"
  PRINT " indicare il numero di cui si desiderano le potenze
  INPUT no

cifre:
  t=10000 : x=8 : y=x+2
  DIM m(x),nn(x),l(y)
  k=1:nn(0) = no : m(0) = no

  FOR i = 1 TO 2
    IF m(i) = t THEN m(i+1) + INT(m(i)/t) : m(i) = m(i) - t *INT(m(i)/t)
    nn(i) = m(i)
  NEXT i

uno:
  CLS
  PRINT "potenze in precisione multipla di " ; no

due:
  k=k+1

  FOR i = 0 TO y
  l(i)=0
  NEXT i

  FOR j = 0 TO 2
    FOR i = 0 TO x
      l(i+j)= l(i+j)+ nn(i)*m(j)
    NEXT i
  NEXT j
```

Un esempio di output del programma: 12763^51 possiede 53 cifre.




```
  FOR i = 0 TO x
    nn(i) = 1(i)
  NEXT i

  FOR i = 0 TO x

    IF nn(i) >= t THEN nn(i+1) = nn(i+1) + INT(nn(i)/t) : nn(i) = nn(i) - t*INT(nn(i)/t)
  NEXT i

  FOR i = 0 TO x
    IF nn(i) > 0 THEN 11 = i
  NEXT i

risultato:
  PRINT no ; " ^ " ; k ; " = " ; STR$(nn(11));

  FOR i = 11-1 TO 0 STEP -1
    u$ = STR$(nn(i))
    j = 4 - (LEN(u$)-1): j1=j
    lb1: IF j1>0 THEN PRINT "0";: j1=j1-1 : GOTO lb1
    PRINT u$;
  NEXT i

  PRINT

  IF k MOD 10 = 0 OR (nn(x)*t + nn(x-1)) * no >= t^2 THEN GOTO tre

  GOTO due

tre:
  PRINT "premere un tasto per avere le successive"
  lb2: k$=INKEY$ : IF k$="" THEN GOTO lb2
  IF (nn(x)*t + nn(x-1))*no >= t*t THEN fine
  GOTO uno


fine:

END
```

Programma per il calcolo di potenze di un numero in multipla precisione: per un corretto output su altre macchine può essere necessario modificare opportunamente i comandi della riga individuata dalla label «risultato» e successive.

di cifre. Il numero di cifre significative che una macchina fornisce in risultato è funzione di una serie di parametri, come architettura della CPU, sistema operativo, linguaggio (certi FORTH ammettono risultati, addirittura, in quintupla precisione), particolare finalizzazione della macchina (la cosiddetta specificità) ecc. Generalmente, comunque, la maggior parte delle macchine, anche dotate di cuori a 16 bit, si fermano alle prime sette-dieci cifre significative, e solo in casi più lodevoli ma meno frequenti si può arrivare alle 12-14 cifre ed oltre; ma anche qui, spesso, pur rimanendo la precisione, la possibilità di visualizzazione è più teorica che reale, visto che, generalmente, le cifre finali vengono tenute in conto dalla macchina, ma non visualizzate.

Comunque, oltre tali barriere, il risultato cade nella trappola dell'arrotondamento e della notazione esponenziale, sistema utile quest'ultimo, ma non sempre capace di risolvere certi particolari problemi, abbisognanti di precisione estrema, fino alla cifra meno significativa.

Occorre, così, scegliere; o comprare una macchina dedicata (ma ce ne sarà poi qualcuna capace di risolvere tutti i problemi?), o ricorrere ad un algoritmo specifico che consenta, anche ad una macchina senza eccessive pretese, di trattare numeri voluminosi senza passare alla notazione scientifica.

A ciò serve l'algoritmo di questa puntata: gli esempi che daremo non possono, ovviamente coprire tutti i casi, ma il nostro scopo è quello di fornire in primis non una soluzione, ma il procedimento risolutivo; ognuno potrà adattarlo alla sua bisogna, a seconda della elasticità dell'algoritmo stesso.

$Y(1) = 34 \qquad Y(0) = 5678$

con ciò, ovviamente, intendendo come X valga

$X(1) \times 10^4 + X(0)$

```
ricordate la vecchia domanda delle medie : quale è il
maggior numero esprimibile con 3 Cifre : La risposta era

9^9^9

il risultato è

196628927832498995095337150220984411756938141727962023364289

(chissà come si legge!)
```

ed Y analogamente risulti pari a

$$Y(1) \times 10^4 + Y(0)$$

Il risultato, semplicemente, sarà (utilizzando la array R):

$$R(0) = X(0) \times Y(0)$$
$$R(1) = X(1) \times Y(0) + X(0) \times Y(1)$$
$$R(2) = X(1) \times Y(1)$$

e, in forma numerica,

$$R(0) = 6543 \times 5678 = 37151154$$
$$R(1) = 87 \times 5678 + 6543 \times 34 = 716448$$
$$R(2) = 87 \times 34 = 2958$$

ed il risultato sarà

$$2958 \times 10^8 + 716448 \times 10^4 + 37151154 = 303001631154$$

Il calcolo con il computer (e con il programma che formiamo) non viene eseguito seguendo esattamente questa strada (anche se il cuore dell'algoritmo è effettivamente questo), perché il calcolatore arrotonderebbe, in fase di elevamento a potenza, e poi di addizione, i risultati; si ricadrebbe, cioè, nella tipologia d'errore iniziale. Il trucco sta nel ridurre R(0) a sole quattro cifre significative (le più a destra), così che

$$R(0) = 1154$$

mentre le altre quattro cifre significative vengono aggiunte
(come addendo) ad R(1)

$$R(1) = 716448 + 3715 = 720163$$

A questo punto ritagliamo le quattro cifre a destra di R(1) ed assegnamole a questa variabile, scaliamo il rimanente a R(2). Avremo, allo stesso modo:

$$R(1) = 0163$$
$$R(2) = 2958 + 72 = 3030$$

A questo punto il risultato è sconta-to (ed esatto fino all'ultima cifra). Per ottenerlo basta legare insieme le tre variabili, in forma di stringa, e leggerle di fila. Vale a dire che

C1&C2&C3 (utilizzando la notazione BASIC ANSI)

darà:

3030|0163|1154

con il pipeline (|) rappresentante l'invisibile punto di giunzione delle diverse variabili.

Il processo, qui esemplificato, per semplicità, con numeri di 6 cifre, è del tutto generico, ovviamente ricordando come occorra ampliare il numero degli elementi della array a seconda delle effettive esigenze (molto meglio se si dispone di un calcolatore che esegue il dimensionamento dinamico delle array).

A titolo esemplificativo di quanto abbiamo appena detto forniamo, a lato un programma che consente di calcolare, in maniera del tutto precisa, potenze successive di un numero in input. Il programma esegue automaticamente potenze del numero dato aumentando, ad ogni ciclo, l'esponente di uno, fino a che raggiunge la lunghezza di 36 cifre: se si desiderano esplorare campi più ampi, occorre cambiare il valore della X nella linea 100; il grado di precisione ottenuto è dato dalla formula [(X+1)*4]: gli esempi e l'output ottenibile dal programma presentano il numero sezionato in blocchi di 4 cifre, a causa della metodologia di funzione dell'algoritmo, che individua stringhe di 4 lettere; poiché Microsoft Basic (e molti altri) inseriscono, prima di stampare una stringa, un blank iniziale, se questa stringa la si ottiene da una conversione di un numero (funzione STR$), il numero appare sezionato in maniera insolita. Niente di più! MC

COMMODORE

Commodore 64 NEW	395.000
Commodore 64 NEW + Registratore	440.000
Commodore 128	**515.000**
Commodore 128 D	**1.160.000**
Drive 1541	405.000
Drive 1571	520.000
Monitor 1801	495.000
Monitor 1901	680.000
Stamp. MPS 803 + tratt.	455.000
Seikosha per 64/128	**380.000**
St. CBM MPS 1000	**655.000**
Registr. comp. 64/128	55.000

Per Accessorie Software COMMODORE telefonare

ATARI 520 STM / 1040 ST

Tastiera 520 ST	699.000
Tastiera 520 ST PLUS	980.000
Tastiera 1040 STF	1.680.000
Drive SF 354	325.000
Drive SF 314	460.000
Monitor SM 124	325.000
Monitor Colore SC 1494	799.000

PACCHETTI ATARI

1 520 ST + 1 SF 354 + 1SM 124	1.310.000
1 520 ST PLUS + 1 SF 354 + 1 SC 1424	1.850.000
1 520 ST PLUS + 1 SF 354 + 1 SM 124	1.525.000
1 1040 STF + 1 SM 124	1.950.000

Software 200 titoli telefonare

LINEA DISITACO PC COMPATIBILI

PC COMPATIBILE
2 DRIVE 360 K
L. 1.590.000 + IVA

PC COMPATIBILE
UN DRIVE 360 + HD 20 MB
L. 2.690.000 + IVA

PC AT COMPATIBILE
HD 20 MB
COMPLETO
L. 3.700.000 + IVA

OLIVETTI M 24
256 K + 2 DISK 360 K
L. 3.600.000 + IVA

OLIVETTI M 24
1 DRIVE 360 K + HD 20 MB
L. 4.900.000 + IVA

Tutte le configurazioni comprendono: CPU 256 K, 2 Drive 360 K, Monitor monoc., DOS, Manuali, Garanzia 1 anno

OLIVETTI PRODEST

Computer 128 K + Registratore	380.000 + IVA
Computer 128 K S + Drive e Monitor	995.000 + IVA

PERIFERICHE PC COMPATIBILI

Disco Rigido Interno 20 MB Slim completo	1.300.000 + IVA
Disco Rigido Interno 30 MB Slim completo	2.100.000 + IVA
Disco Rigido Esterno 20 MB completo	1.850.000 + IVA
Back up a nastro Irwin 20 MB interno	1.699.000 + IVA
Modem IBM comp.	350.000 + IVA
Espansione 640 K RAM	230.000

DATA GENERAL
IBM COMPATIBILE
PORTATILE
L. 3.200.000 + IVA

FAVOLOSO SISTEMA VIDEOSCRITTURA AMSTRAD
Monitor, Drive,
Tastiera 256 K, Stampante
L. 1.390.000 + IVA

SINCLAIR

Sinclair QL versione italiana	**499.000**
Monitor QL 14" colore	570.000
Interfaccia parallela	99.000
Disk drive per QL 1 MB	580.000
Drive 2 aggiuntivo 1 MB	345.000
Mouse per QL	210.000
ZX Spectrum 2 128 K (reg. incorporato)	**440.000**

Per accessori e software Sinclair telefonare

PACCHETTI QL

QL + Drive 1 + valigetta QL	1.100.000
QL + Drive 1 St. Epson LX 80	1.699.000
Drive 1 + Drive agg.	799.000

COMMODORE AMIGA

Commodore AMIGA 512 K + Monitor colore pronta consegna	telefonare
prezzo eccezionale Video digitizer + telecamera	900.000 + IVA

Drive aggiuntivo 1 MB	740.000
Sidecar M.S. DOS	in arrivo
Esp. 2 MB	in arrivo

Software oltre 150 titolitelefonare

STAMPANTI

Mannes. Tally MT 80 PC	680.000
Mannes. Tally MT 85	960.000
Mannes. Tally MT 86	1.180.000
Mannes. Tally MT 290	**1.899.000**
CBM MPS 1000	655.000
Epson LX 80 F/T	749.000
Epson FX 105	**1.250.000**
Seikosha GP 500 VC	380.000
Citizen 120 D IBM	680.000
Citizen 120 D CBM/64/128	699.000
Stampante per Spectrum	280.000

MONITORS

Mon. Hantarex X12	199.000
Mon. Hantarex B12	230.000
Mon. colore 1801	495.000
Mon. colore 1901	680.000
Mon. QL colore	570.000
Mon. IBM comp.	280.000
Mon. Hant. colore	570.000

DIREZIONE SERVIZI COMMERCIALI:
Via Arbia, 62
tel. 857607-8440766-867741

GRUPPO DISITACO

***Assistenza Tecnica curata da:* DCS ITALIA**
Via Arbia 62, tel. 06/ 867742

TUTTI I PRODOTTI SONO COPERTI DA GARANZIE UFFICIALI NAZIONALI

PUNTI VENDITA

COMPUTRON SHOP
L.go Forano, 7/8 - Tel. 8391556
(Salario, Parioli)

COMPUTER FRIEND
Via Antonazzo Romano, 3
Tel. 393321
(Flaminio, Monte Mario)

2 M ELETTRONICA s.r.l.
Via Britannia, 17 - Tel. 7550935
(S. Giovanni, Appio Latino)

BIT HOUSE s.r.l.
V.le Kennedy, 100 - Tel. 9005815
(Monterotondo)

DISITACO s.r.l.
Via Massaciuccoli, 25/A
Tel. 8390100
(Trieste, Nomentano)

I.C.P. s.r.l.
Viale Cetra, 24-26
Tel. 0773-486977 **(Latina)**