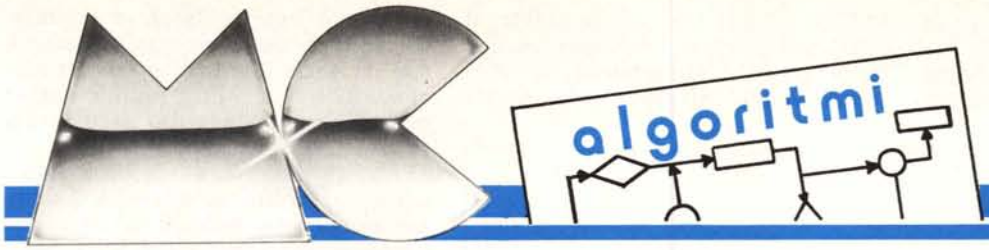

di Raffaello De Masi

Massimo Comun Divisore Minimo Comune Multiplo Numeri primi

Seconda parte

Ah, bei tempi di scuola media; che sapore hanno oggi le scomposizioni in fattori, le potenze, le espressioni! Quanto ci ha fatto sudare questo Massimo, che, lungi dall'essere così divertente come sosteneva la nostra insegnante di matematica (vecchia e zitella, poteva non essere?), ci imponeva l'elucubrazione mentale del «prodotto di tutti i fattori, comuni e non comuni, presi, come se ci fosse qualcuno che volesse prenderli, una sola volta con il minimo esponente».

Oggi questo massimo (che però era più piccolo, accanto al suo avversario «minimo» che invece era a lui maggiore; perdonate il gioco di parole), ci fa sorridere e ci fa ripensare alla compagna di banco oggi mamma di quattro bimbi, al «filone» (così si chiama dalle mie parti il deamicisiano marinare la scuola), alla compravendita di libri usati ed ai verbi difettivi. Il tempo è passato, ma il massimo dei divisori comuni rimane ancora un babau della prima media, e non pare voler dar segno di andare in pensione o di addolcire la sua immagine di castigatore di alunni svogliati e disattenti.

Visto che ci siamo, e nonostante il continuo aggiornamento dei programmi ministeriali ed anticipando la prossima rivoluzione informatica presente che si prevede riaccenderà il fuoco un po' deboluccio della scuola, perché non gettare questo mostro sacro nell'arena di silicio, e vedere se riescono a sbrogliarsela tra di loro, lui e la CPU?

Se A e B sono ambedue numeri interi, si definisce divisore comune (o comune fattore) un intero che divide ambedue i numeri senza resto. Il più grande di tali fattori rappresenta il nostro, Il Massimo Comun Divisore (o più correntemente il M.C.D., scritto in maiuscolo, per evidenziare la sua differenza col m.c.m.). Così 24 e 36 hanno come divisori 2 e 4, ma possiedono un unico M.C.D., 12.

La ricerca classica, lo ricordiamo tutti, era basata sulla ricerca dei minimi divisori dei due numeri; dal confronto di essi veniva ricavato un prodotto di fattori comuni che forniva il dato ricercato.

Il metodo scolastico non è particolarmente adatto ad essere sviluppato da un computer. Ciò nonostante esistono altri metodi, più congeniali ad un calcolatore, che consentono di ricavare efficacemente ed elegantemente il dato ricercato. Particolarmente adatta alla tipologia di calcolo di un computer è una regola piuttosto antica, forse quella più vecchia conosciuta (III secolo a.C.), che viene attribuita ad Euclide, e da lui prende il nome di algoritmo euclideo.

Si abbiano due numeri A e B di cui si cerchi il M.C.D.; sia A maggiore di B (opzione piuttosto semplice da rendere con un calcolatore); R, sia il resto della divisione A/B, vale a dire

$$R_1 = A \bmod B$$

o, il che è lo stesso

$$R_1 = A - B \cdot \mathrm{int}(A/B)$$

Per sua stessa definizione (minimo sottomultiplo di A e B), ogni numero che divide contemporaneamente A e B sarà anche divisore di R_1, e per proprietà transitiva, potremo affermare che ogni comune divisore di B ed R_1 sarà anche divisore di A. Come conseguenza i divisori comuni di A e B saranno gli stessi di B ed R_1 e la ricerca dei primi potrà essere convenientemente ridotta a quella dei secondi.

A questo punto dividiamo B per R_1 e leggiamo il resto R_2, vale a dire:

$$R_2 = B - R_1 \cdot \mathrm{int}(B/R_1)$$

Quanto espresso precedentemente lo applicheremo ancora qui; in particolare, la ricerca del M.C.D. di A e B potrà essere ricondotta a quello di R_1 ed R_2.

Continuiamo con il processo; troveremo R_3 come resto di:

$$R_3 = R_1 - R_2 \cdot \mathrm{int}(B/R_1)$$

e così via fino ad ottenere il resto di zero.

Il processo non è indefinito; infatti, poiché i rapporti (ed i resti) sono riferiti a cifre sempre più piccole, si giunge, alla fine, al resto di 0. In tal caso il resto della divisione precedente a quella che ha dato un quoto rappresenta il massimo comune divisore dei due numeri A e B.

Il processo, ripetitivo com'è, e, d'altro canto, notevolmente semplice nella impostazione (nel listato allegato occupa non più di cinque righe) si presta ad essere affrontato con notevole efficienza da un computer. Ne diamo, a pagina 108, un listato esemplificativo.

Quanto finora detto vale anche, ov-

viamente, per la ricerca del M.C.D. di più numeri; la soluzione è ovvia; basta sviluppare l'operazione per coppie di numeri per ottenere una serie di M.C.D. relativi alle coppie stesse; il calcolo di un nuovo massimo comune fattore tra i risultati ottenuti darà il risultato voluto. All'atto pratico risulta più conveniente confrontare il risultato ottenuto dalla ricerca precedente con un nuovo numero, e così via fino al risultato finale. Ed è proprio questo procedimento che viene seguito dal programma presentato.

Ancora una cosa: il programma consente, inoltre, di calcolare il minimo comune multiplo (il minor valore contemporaneamente divisibile per i numeri di partenza) dei numeri inseriti: l'algoritmo utilizzato, peraltro banale e del tutto intuitivo, è rappresentato dalla formula:

A•B•C ... •N/ (Massimo Comune Divisore)$^{(n-1)}$

dove n rappresenta il numero dei valori oggetto di ricerca.

```
'                    MASSIMO COMUNE DIVISORE
'                    E MINIMO COMUNE MULTIPLO
'
'
'       attenzione : il dimensionamento della array N è eseguito dinamicamente
'       non sempre tale procedura è ammessa su altre macchine

  CLS

zero:
  PRINT"          Il presente programma consente di calcolare il massimo"
  PRINT"       comune divisore ed il minimo comune multiplo di due numeri"
  PRINT"              utilizzando il cosiddetto algoritmo euclideo"
  PRINT
  flag=0:flag1=0
  PRINT"inserire i valori richiesti"
  PRINT
  INPUT" di quanti numeri occorre calcolare il M.C.D." ,z
  IF z<2 THEN PRINT "per favore , non fare lo stupido" : GOTO zero

  DIM N(z)

uno:
  FOR x = 1 TO z

unob:
  PRINT " indicare il ";x;"° numero"
  INPUT N(x)
  IF N(x) < 0 OR N(x) <> INT(N(x)) THEN x = z : PRINT " attenzione , per favore" : GOTO unob
  NEXT x

due:
  N(0)= N(1) : a = N(0)

tre:
  FOR k = 2 TO z

  a=N(0) : b=N(k)

trea:
  IF a < b THEN c=b : b=a : a=c
  flag=1
  resto = a - b * INT(a/b)              in alternativa resto = a mod b
  IF resto <> 0 THEN a = b : b = resto : flag = 0
  IF flag THEN treb




  GOTO trea

treb:
  N(0)=b
  NEXT k

quattro:
  CLS
  IF b > 1 THEN quattroa
  PRINT " Spiacente : i numeri sono primi tra di loro"
  PRINT " il loro massimo divisore comune è l'unità": GOTO cinque

quattroa:
  PRINT"il massimo comune divisore di "

  FOR k = 1 TO z
  PRINT N(k)
  NEXT k

  PRINT
  PRINT " è " ; b

cinque:
  cc=N(1)
  FOR k = 1 TO z-1
  cc=cc*N(k+1)
  NEXT k
  c=cc/(b^(z-1))
  PRINT
  PRINT"il minimo comune multiplo è"  ";c
  END
```

Figura 1 - Ricerca del Massimo Comune Divisore e del minimo comune multiplo con l'algoritmo euclideo.

Numeri Primi

Il Crivello di Eratostene

Chi ci ha seguiti finora si sarà reso conto che quanto svolto rappresenta una specie di collezione di tool, utility di base che ci serviranno in seguito per sviluppare argomenti molto più impegnativi. Ciò nonostante, ognuno degli argomenti finora mostrati (e degli algoritmi in essi espressi), può essere ovviamente guardato come argomento di puro interesse speculativo.

In tale ottica va inserito l'argomento successivo, che sebbene utile per molti dei campi che svilupperemo nei prossimi numeri (calcolo di determinanti e matrici, serie, ecc.) ci consente, però, di riandare, ancora una volta, a sederci tra i banchi di scuola per rivedere, in chiave informatica, un classico argomento di una ancora più classica aritmetica di scuola media.

Si intende come primo un numero intero positivo, diverso da uno, non divisibile per alcun altro numero intero, ad esclusione dell'unità e di se stesso (per essere precisi dovremmo, in verità, dire esattamente divisibile). Così i numeri 2, 3, 5 e 23 sono primi, mentre non lo sono 4, 6 e 2.000.

Non esiste, o non è stata ancora scoperta, una formula generale per il calcolo immediato dei numeri primi; Euclide, ancora lui, per primo dimostrò che essi sono infiniti e notò come, coll'aumentare del valore dei numeri, essi si diradino sempre più, pur non essendo mai, nella loro distribuzione, regolari e prevedibili. L'interesse verso i numeri primi, comunque è stato costante nel tempo (se ne è interessato, in maniera massiccia ed impegnata, addirittura il grande Gauss), e, in questo secolo ha riassunto di nuovo una notevole attenzione da parte degli studiosi per la utilizzazione abbastanza spinta di essi nel campo della crittografia e dei codici segreti di trasmissione.

Qualche precisazione riguardo ai listati presentati

Essi sono relativi alla versione Microsoft Basic implementata su Apple Macintosh. La loro lettura non presenta alcunché di particolare, ad esclusione del fatto che non compaiono i numeri di linea, che in questa implementazione sono inutili. I punti nodali del programma, necessari per l'indirizzamento dei salti e delle sbr, vengono localizzati da etichette (nei listati rappresentate da «uno», «due», ecc.) che si distinguono per essere immediatamente seguite dai due punti (:). L'apostrofo (') sostituisce il più noto REM mentre viene lasciato l'END, qui superfluo, ma necessario in quasi tutte le altre implementazioni del Basic. Le Keyword appaiono in grassetto, ma sono, a tutti gli effetti, corrispondenti a quelle di qualsiasi altro Basic. Proprio per evitare confusione si è preferito non utilizzare, per quanto possibile, statement specifici della macchina in questione e dello specifico linguaggio implementato. Nel caso, successivamente, occorresse far ricorso a procedure particolari, non mancheremo di evidenziare la cosa, e di darne opportuna spiegazione.

Ancora, in ambedue i programmi si fa uso della tecnica di dimensionamento delle variabili in forma dinamica; in parole più povere e meno auliche, le array vengono dimensionate non in modo fisso, ma in base alla nostra effettiva necessità, rappresentata, generalmente, dal valore di una variabile in input. Qualora ciò non fosse possibile sulla vostra macchina, occorrerà inserire volta per volta nel programma il dimensionamento necessario.

```
'                    CRIVELLO DI ERATOSTENE
'
'
'                 questo programma consente il calcolo
'                     dei numeri primi compresi
'                   tra 2 ed un numero arbitrario
'
'
'
zero:
     CLS
     PRINT"Questo programma consente di calcolare i numeri primi"
     PRINT"compresi tra 2 ed un numero N"

'    attenzione , i numeri oggetto di analisi verranno inseriti in una array
'    per tale motivo occorre tener conto della memoria disponibile e
'    dimensionare la variabile a(n) in funzione della disponibilità esistente
'
'    molte macchine non ammettono il dimensionamento dinamico di una array
'    pertanto occorrerà sostituire alla variabile n dello statement DIM a(n)
'    l'effettivo valore del numero cercato


uno:
     PRINT
     INPUT "Indicare il limite massimo di ricerca";n
     IF n < 3 AND n<> INT(n) THEN PRINT " non fare lo stupido " : GOTO uno

due:
     DIM a(n)
     CLS
     PRINT " I primi compresi tra 2 e ";n;" sono :"
     WIDTH 60                    'definisce l'ampiezza della linea di output
                                 ' inutile su altri computer
     PRINT

     FOR i = 2 TO n
tre:
     IF a(i) = 0 THEN GOSUB dieci

     NEXT i

fine:
     END

'  ----------------


' 1° subroutine


dieci:
     PRINT " ";i;" ";
     FOR j= i TO n STEP i
     a(j)=1
     NEXT j

     RETURN
```

Figura 2 - Il listato della ricerca dei numeri primi utilizzando il Crivello di Eratostene. Si noti il dimensionamento dinamico della array a(n).

Il metodo (attenzione, non la regola), più efficace per la individuazione dei numeri primi da 2 ad N (inteso, questo, come valore superiore del campo di numeri investigati), è rappresentato dal Crivello di Eratostene (di Cirene, matematico greco vissuto dal 276 al 196 a.C., cui si deve il primo calcolo della circonferenza della terra). Il procedimento si basa sullo scrivere tutti i numeri interi da 2 ad N, quindi partendo da 2 cancellare tutti i numeri ad intervalli di 2. Esaurita l'operazione, il numero successivo al 2 (nel caso particolare il 3) sarà primo. Dopo di ciò, partendo dal 3 si cancellano tutti i numeri ad intervalli di 3 (ovvio che sarà possibile cancellare di nuovo numeri eliminati già nella precedente ricerca). Ancora, al termine dell'operazione, il numero successivo a 3 e non cancellato (5) sarà primo. Partendo da questo, elimineremo ancora tutti i numeri ad intervalli di 5, e così via. Al termine dell'operazione, i numeri rimasti saranno primi.

Il procedimento qui esposto, senz'altro faticoso e noioso da eseguire a mano, è efficacemente e facilmente trasformabile in un programma (che viene presentato in questa stessa pagina.

Esso chiede in input un valore e fornisce tutti i primi compresi tra 2 ed il valore stesso.

È più che ovvio che una semplice modifica del programma consentirà di calcolare i primi compresi tra N ed N1.

Il listato è piuttosto semplice da leggere e non abbisogna di soverchi commenti; diremo solo che l'esecuzione rallenta moltissimo quando il range è piuttosto ampio. La ricerca dei primi compresi tra 2 e 10.000, utilizzando il listato che leggete su un Macintosh dotato del più recente Microsoft Basic (il 2,1), è durata, compreso l'output sullo schermo, ben 2 minuti e 33 secondi, mentre un Hewlett-Packard, 87, ben più versato del Mac in questo campo di applicazione, non è comunque sceso al di sotto del minuto e mezzo.

Il Crivello di Eratostene è concettualmente semplice, ed è utile per avere una lista dei numeri primi compresi tra due valori.

Ma non è un metodo pratico per verificare se un certo numero è primo (immaginate di eseguire un test del genere per determinare se 987654323 è primo o no; ci sarebbe da far vacillare la mente più salda, nell'attesa davanti allo schermo); esistono metodi più efficienti per risolvere questo problema; ne riparleremo la prossima volta; comunque, se proprio non ce la fate ad aspettare, possiamo almeno svelarvi che il numerone precedente è primo; a risentirci. MC