LABORATORIO DI ALGORITMI
DISPENSE

Capitolo 1: Introduzione

Consideriamo la seguente successione $\{a_i\}$ di numeri razionali in cui $a_0 = 1$ e $a_{i+1} = \frac{m_{i+1}}{n_{i+1}} = \frac{m_i + 2n_i}{m_i + n_i}$:

(1) $$\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \ldots$$

Confrontiamo i valori così ottenuti con $\sqrt{2}$.

Non solo sono una buona approssimazione ma la successione (1) fornisce una approssimazione estremamente precisa: infatti $a_i - \sqrt{2} < \frac{1}{2n_i}$.
Questo algoritmo era già noto ai tempi dell'antica Grecia. Invece un algoritmo assai più recente, che ha meno di 150 anni per intenderci, è il seguente test atto a verificare se, dato un intero dispari $n > 1$, il numero $m = 2^n - 1$ è primo oppure no.

Si ponga $S = 4$ e si ripeta $n - 2$ volte il seguente ciclo di operazioni: calcolare $S^2 - 2$, dividere il risultato per m e assegnare a S il resto della divisione.
Alla fine dei cicli si ispezioni il valore assunto da S: se è nullo allora m è primo, viceversa no.

Nel 1999 questo algoritmo è stato utilizzato per verificare se $2^{6.972.593} - 1$ è primo battendo così il record per il più grande numero primo conosciuto sulla Terra.

Questi due algoritmi, appartenenti a due epoche lontane tra loro, sono due tra gli algoritmi di teoria dei numeri.

Ma che cos'è la Teoria dei Numeri? Teoria dei Numeri è quella disciplina della Matematica che si occupa dello studio delle proprietà dei numeri interi ed è da lungo tempo inseparabile dagli algoritmi: per individuare degli algoritmi efficienti è indispensabile comprendere la struttura degli interi e tale esplorazione è facilitata dallo studio degli algoritmi già noti.

La fattorizzazione di numeri interi molto grandi offre un esempio della necessità di comprendere tale struttura.

Si pensi che, grazie ai recenti algoritmi, oggi è possibile fattorizzare numeri interi costituiti da un centinaio di cifre in maniera ordinaria.

A prima vista sembrerebbe banale, sfruttando un approccio metodologico e un congruo numero di elaboratori potenti, procedere con l'elencazione dei numeri primi inferiori al numero da fattorizzare e poi semplicemente proseguire per tentativi dividendo il numero per ogni primo della lista nella speranza di pervenire a un resto nullo.

Come vedremo generare la lista dei potenziali fattori primi non è compito arduo. Il problema è che di potenziali divisori ce ne sono una quantità enorme!

Ad esempio se il più piccolo divisore primo del nostro numero è costituito da 50 cifre (e oggigiorno un numero siffatto non è considerato poi così grande) allora un teorema sui numeri primi afferma che dovremo effettuare circa 8.7×10^{47} tentativi prima di individuare un fattore!

Immaginando un processore ideale che sia in grado di elaborare 10^{12} divisioni al secondo, se mettessimo in parallelo 10^{6} di questi processori, noi saremmo in grado di testare 10^{18} primi differenti al secondo.

Sembrerebbe interessante... ma non è così!

Infatti ci sono circa 3.2×10^{7} secondi in un anno dunque sarebbero necessari più di 10^{22} anni per completare la fattorizzazione!

Tanto per dare un'idea, si stima che l'universo abbia poco meno di 2×10^{10} anni...