PROGRAMMAZIONE DI SISTEMI MULTICORE

Fattorizzazione numeri RSA
Giuseppe Costantino

I numeri RSA sono numeri semiprimi facenti parte del RSA Factoring Challenge creata dai RSA Laboratories.

FUNZIONI AUSILIARIE

SIZE
Prende in ingresso un array e lo scansiona fino a che non incontra un valore nullo. Nel main viene utilizzata per calcolare la dimensione dell'array che contiene i fattori di un dato numero, quindi il valore nullo ne segnerà senza dubbio la fine.

PRINT
Prende in ingresso un array e sfruttando la funzione size ne stampa tutti gli elementi.

PRIMO
Dato un intero restituisce se è un numero primo o meno. Tramite un ciclo for conta il numero di divisori di quel numero. Se è esattamente 2 allora è un numero primo (il ciclo va da 1 al numero compresi), altrimenti no.

FACT
Calcola i fattori primi di un numero dato in un range tra 3 e il numero stesso escluso. L'iteratore i viene incrementato di 2 (i+=2) per considerare solo I numeri dispari. Restituisce l'array di tutti i fattori controllando prima che siano numeri primi.

FUNZIONE MAIN
Prende il numero da fattorizzare tramite linea di comando e viene convertito in intero tramite la funzione atoi.
L'apertura dell'ambiente MPI (così come la chiusura) viene controllata da MPI_SUCCESS.
La funzione MPI_Comm_size restituisce il numero di processi, MPI_Comm_rank l'id di ognuno di questi, MPI_Barrier blocca l'esecuzione di ogni processo fino a che ognuno di essi non ha completato la sua esecuzione.
In particolare, vengono utilizzati 4 processi.
Il primo (id==0) invia il numero dato in ingresso ai rimanenti 3 processi; il secondo controlla che non sia un numero primo; il terzo ne calcola I fattori e li stampa, il quarto controlla che sia un numero RSA.

Per la gestione dei numeri arbitrariamente grandi si utilizza la libreria ufficiale GNU GMP(https://gmplib.org/).

COMPILARE ED ESEGUIRE

-mpicc nomefile.c -o nomeExe

-mpiexec -n N ./nomeExe num
N=numero processi
num=numero da fattorizzare