Programmazione Cl.B

Andrea Piroddi

Dipartimento di Informatica, Scienza e Ingegneria

Elaborato 4 - is_prime

```
unsigned short int is_prime(unsigned short int n) {
        if (n == 2) {
                return 1;
        }       if (n == 0 || n == 1 || n % 2 == 0) {
                return 0;
                }
        else {

Piccolo Teorema di Fermat
        }
}
```

/* Ritorna 1 se n e' primo, 0 altrimenti. */

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

Elaborato 4 - is_prime

Un procedimento per scoprire se si tratta di un numero primo è il "Piccolo Teorema di Fermat (PTF)", dovuto a Pierre de Fermat e dimostrato successivamente da Eulero.

Risulta essere un metodo antichissimo ma ancora valido, utilizzato già nel XVII secolo, che conserva ancora il suo fascino.

È quasi sempre tirato in ballo, anche nei nuovi metodi di primalità come AKS.

Il piccolo Teorema di Fermat dice che se n è un numero primo, allora per ogni intero a è verificato che:

$$a^n \equiv a \ (mod \ n)$$

Questo significa che se si prende un qualunque numero a, lo si moltiplica per se stesso n volte, il risultato è divisibile per n.

Elaborato 4 - nth_prime

```
unsigned short int nth_prime(unsigned short int n) {
unsigned int count = 0, prime = 2, i;


for (i = 3; i <= USHRT_MAX && count < n; i++)
…


return count == n ? prime : 0;
}
```

Ritorna l'n-esimo primo, contando a partire da 0.
Se il numero e' troppo grande per essere rappresentato con un unsigned short int, ritorna 0.

Elaborato 4 - nth_prime

USHRT_MAX costante macro dell'header *limits.h* in C.

Viene utilizzato per ottenere il valore massimo di un oggetto ***unsigned short int***, restituisce il valore massimo che può memorizzare un oggetto ***unsigned short int***, che è 65535 $(2^{16} - 1)$.

Elaborato 4 - succ_prime

```
unsigned short int succ_prime(int reset) {
static unsigned short int prime = 0;

if (reset != 0 || prime == 0) {
                prime = 2;
                }
else if (prime == 2) {
                prime = 3;
                }
else {
unsigned long int i;

for (i = prime + 2; i <= USHRT_MAX && !is_prime(i); i += 2);

…

return prime;
}
```

Ritorna la successione di numeri primi.

La prima chiamata ritorna 2, la seconda 3, ecc.

Se il parametro reset e' diverso da 0, allora la successione viene resettata e la funzione ritorna 2.

Diversamente, la funzione ritorna il primo successivo a quello ritornato alla chiamata precedente.

Se il primo successivo e' troppo grande per essere rappresentato con un unsigned short int, la funzione ritorna 0 e la successione viene resettata.

Elaborato 4 - co_prime

/* Ritorna 1 se m e n sono coprimi, 0 altrimenti. */

```
unsigned short int co_prime(unsigned short int m, unsigned short int n) {
unsigned int i, x = m < n ? m : n;


if (m % 2 == 0 && n % 2 == 0)
return 0;


...
}
```