# SUI NUMERI PRIMI

Un numero primo, in matematica, è un numero naturale divisibile unicamente per se stesso e per l'unità e diverso, per convenzione, dall'unità.
Detto in altro modo, deve avere esattamente due fattori distinti di cui uno è l'unità.
La loro importanza in matematica è enorme e deriva dal teorema fondamentale dell'aritmetica, il cui enunciato è:

*" Qualsiasi numero può essere scomposto in fattori primi, e tale scomposizione è unica "*

Possiamo quindi dire che i numeri primi sono i mattoni con cui costruire tutti i numeri naturali, gli atomi dell'aritmetica. Pertanto una migliore conoscenza dei numeri primi porta a progressi in tutta quella branca della matematica che va sotto il nome di "Teoria dei numeri".
Ma il vero impiego dei numeri primi è soprattutto in campo telematico e crittografico.
Infatti trovare i fattori di un numero intero molto grande è una impresa assai ardua, e può essere considerata quasi impossibile date le risorse disponibili. Per questo motivo possono essere impiegati in alcuni sistemi di crittografia come la famosissima cifratura RSA ( con cui possiamo svolgere operazioni bancarie o anche più semplicemente acquisti on-line in maniera sicura ) in cui viene affrontato il problema della fattorizzazione di un numero molto grande.
Per questi motivi oggi si è alla ricerca di nuovi metodi per calcolare numeri primi sufficientemente grandi .
Fra questi trova largo impiego l'algoritmo di Mersenne che non sempre però produce numeri primi.
Esso si presenta in questa forma :

$$M_{(p)} = 2^p - 1$$

In cui *p* è un numero primo.
Se $M_{(p)}$ è primo si dice numero primo di Mersenne, altrimenti si dice numero di Mersenne.
I primi numeri primi di Mersenne sono 2, 3, 5, 7, 13, 17 …
Infatti come si può notare dalla tabella :

$$M_2 = 2^2 - 1 = 3$$
$$M_3 = 2^3 - 1 = 7$$
$$M_5 = 2^5 - 1 = 31$$
$$M_7 = 2^7 - 1 = 127$$
$$M_{13} = 2^{13} - 1 = 8191$$
$$M_{17} = 131071$$

sono tutti numeri primi.
Se $M_{(n)}$ è primo, allora anche n è primo. Invece n primo non garantisce che $M_{(n)}$ sia primo.
Infatti:

$$M_{(11)} = 2^{11} - 1 = 2047 = 23 * 89$$

Quindi il problema fondamentale dei numeri di Mersenne è quello di testare la primalità di essi.
Come già detto in precedenza la fattorizzazione di un numero, ossia la ricerca dei suoi fattori, è qualcosa di abbastanza impegnativo a tal punto da tenere occupati , per numeri molto grandi, i migliori supercomputer in commercio per periodi di tempo impressionanti che possono arrivare anche a svariati anni.

Per affrontare il problema lateralmente, ossia evitando il problema della fattorizzazione, numerosi matematici si sono cimentati nella ideazione di test di primalità sempre più efficienti e affidabili.
Tra questi il più importante e il più semplice , dal punto di vista della complessità di calcolo, è il test di Lucas – Lehmer.

L'idea principale del test di Lucas – Lehmer è quella di trovare un numero che fosse multiplo del numero di Mersenne. Infatti essendo $L_{(n)}$ multiplo $M_{(n)}$ , *n* è necessariamente primo.

In origine il test, ideato da Lucas presentava grosse difficoltà di calcolo poiché il numero $L_{(n)}$ cresceva in una maniera esponenziale, e grazie alla modifica apportata da Lehmer fu possibile calcolare $L_{(200)}$ con estrema semplicità.

Secondo il test L-L, *p* è primo se e solo se:

$$L_{(p)} \bmod M_{(p)} = 0 \qquad (1)$$

**Il calcolo di $L_{(p)}$**

Per calcolare $L_{(p),}$ bisogna prendere in considerazione il valore precedente :

$$L_{(p)} = (L_{(p-1)})^2 - 2 \qquad (2)$$

Tenendo in considerazione come valore iniziale $L_{(1)} = 4$.
Dato che ci sono alcuni matematici che attribuiscono a $L_{(0)}$ il valore 4, ho pensato al seguente metodo per evitare dubbi e quindi errori :

Se $L_{(x)} = 4$ e si vuole calcolare $L_{(p)}$, il nuovo valore di $L_{(p)}$ , $L_{(p,)}$ , sarà dato dalla formula:

$$L_{(p,)} = L_{(p+x)-2}$$

**Alcuni esempi**
Si vuole testare la primalità del numero di Mersenne, $M_{(5)} = 31$.

Se prendiamo in considerazione come valore iniziale $L_{(1)} = 4$, dobbiamo calcolare:

$$L_{(p,)} = L_{(5+1)-2} = L_{(4)}$$

Quindi tenendo in considerazione la (2) e calcolando il valore di $L_{(4)}$ si ha:

$$L_{(1)} = 4 \bmod 31 = 4$$
$$L_{(2)} = (L_{(2-1)})^2 - 2 \bmod 31 = 14 \bmod 31 = 14$$
$$L_{(3)} = (L_{(3-1)})^2 - 2 \bmod 31 = 194 \bmod 31 = 8$$
$$L_{(4)} = (L_{(4-1)})^2 - 2 \bmod 31 = 62 \bmod 31 = 0$$

$M_{(5)} = 31$ è primo.

Per verificare l'effettiva efficienza del test procediamo nel testare un numero di Mersenne che non sia primo, ad esempio $M_{(4)} = 15$.

Si vuole testare la primalità del numero di Mersenne, $M_{(4)} = 15$.

Se prendiamo in considerazione come valore iniziale $L_{(1)} = 4$, dobbiamo calcolare:

$$L_{(p,)} = \quad L_{(4+1)-2} = L_{(3)}$$

Quindi tenendo in considerazione la (2) e calcolando il valore di $L_{(3)}$ si ha:

$$L_{(1)} = 4 \bmod 15 = 4$$
$$L_{(2)} = (L_{(2-1)})^2 - 2 \bmod 15 = 14 \bmod 15 = 14$$
$$L_{(3)} = (L_{(3-1)})^2 - 2 \bmod 15 = 194 \bmod 15 = 14$$

$M_{(4)} = 15$ non è primo.