Le formule per i numeri primi

I numeri primi, come già sappiamo sono quei numeri naturali maggiori di 1 che sono divisibili solo per se stessi e per l'unità; il primo di essi è 2, che è anche l'unico numero primo pari, gli altri sono tutti dispari: 3, 5, 7, 11, 13, 17, 19, ...
I puntini sono d'obbligo perchè i numeri primi sono tanti, tantissimi, addirittura infiniti; purtroppo però non esiste una regola che li possa generare tutti, o meglio, se una regola c'è, questa non è ancora stata trovata.
Ci sono però dei metodi, alcuni semplici, altri più complessi, che permettono di generarne un po'; fra tutti il **crivello di Eratostene** è sicuramente quello più conosciuto e forse ne avrai già sentito parlare. Funziona così:

- si scrive la successione dei primi n numeri naturali a partire da 2; per ragioni ovvie di spazio scriviamo solo i primi 50

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

- Eliminiamo tutti i multipli di 2, escluso il 2 che è primo

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	

- Eliminiamo adesso tutti i multipli di 3, escluso il 3 che è primo

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	

Proseguendo nello stesso modo, eliminiamo i multipli del primo numero che è ancora nella tabella dopo quello che è stato considerato per ultimo, fino a che non si elimina più alcun numero.
Ecco i passaggi:

- si eliminano i multipli di 5

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	

- si eliminano i multipli di 7

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			

- si eliminano i multipli di 11

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			

A questo punto, poiché in questo passaggio non abbiamo fatto più eliminazioni, la tabella contiene solo numeri primi.

Ci sono altri modi per ottenere numeri primi, basati su delle formule, che però funzionano fino a un certo punto; le più note sono:

- **la formula di Fermat** $F(n) = 2^{2^n} + 1$
  che genera numeri primi solamente per $n = 1, 2, 3, 4$:
  $F(1) = 2^2 + 1 = 5$
  $F(2) = 2^4 + 1 = 17$
  $F(3) = 2^8 + 1 = 257$
  $F(4) = 2^{16} + 1 = 65537$
  ma già per $n = 5$ il numero ottenuto non è primo:
  $F(5) = 2^{32} + 1 = 4294967297 = 641 \times 6700417$

- le formule

  $F(n) = n^2 - n + 41$ e $F(n) = n^2 - 79n + 1601$

  che generano parecchi numeri primi: la prima funziona per tutti gli $n < 40$, la seconda per tutti gli $n < 80$, ma poi vengono generati numeri composti.

Sono stati poi dimostrati diversi teoremi sui numeri primi, alcuni di semplice comprensione, altri invece più difficili per le nostre attuali conoscenze; per esempio si sa che:

- ogni numero primo si può scrivere nella forma $4n - 1$ oppure $4n + 1$, dove n può essere un numero naturale qualsiasi.
  Questa però non è una formula per generare numeri primi perché, per esempio, se $n = 1$ le due formule danno rispettivamente i numeri 3 e 5, se $n = 2$ i numeri generati sono 7 e 9 dei quali però 9 non è primo.
  Essa afferma tuttavia che ogni numero del quale si sa già che è primo si può scrivere come $4n - 1$ oppure $4n + 1$; per esempio:

  $13 = 4 \cdot 3 + 1$

  $17 = 4 \cdot 4 + 1$

  $47 = 4 \cdot 12 - 1$

Ma il problema più importante è un altro: dato un numero qualsiasi (ovviamente dispari) come si fa a sapere se è o non è primo? E ancora, se un numero non è primo, come si fa a trovare i fattori della sua scomposizione?
Un metodo molto semplice è quello basato sulle divisioni; se vogliamo sapere se un numero n è primo cominciamo a dividerlo prima per 2, poi per 3, poi per 4, per 5, per 6 e così via, almeno fino a $\frac{n}{2}$; se nessuna delle divisioni ha dato resto zero possiamo concludere che il numero è primo. In realtà non occorre arrivare fino a $\frac{n}{2}$, basta fermarsi a $\sqrt{n}$; per esempio, per decidere con questo metodo se 20587319 è primo basta fare $\sqrt{20587319}$, cioè 4537 divisioni.
Se poi da questi numeri togliamo tutti quelli pari che sicuramente non sono primi perché divisibili per 2, il numero di divisioni si riduce ancora ma è sempre un numero abbastanza elevato.
È pur vero che i calcoli li fa un computer e che quindi non ci dovremmo preoccupare più di tanto. Pensiamo però ad un numero grande, per esempio $n = 2^{127} - 1$ che è un numero che ha 39 cifre; visto che $\sqrt{n}$ è dell'ordine di 10^{19}, quanto impiegherebbe un computer per fare 10^{19} divisioni?
Un computer con un processore veloce può fare circa 10^{10} operazioni al secondo e, se ne deve fare 10^{19} impiega un tempo pari a $10^{19} : 10^{10} = 10^9$ secondi, cioè

$$10^9 : (60 \times 60 \times 24 \times 365) \approx 31{,}7 \text{ anni;}$$

un po' troppo tempo!
I test di primalità che usano oggi i computer sono molto più efficienti di questo (e molto più complessi per le nostre conoscenze) ed in effetti se imposti la funzione $prime(2^{127} - 1)$ con un qualsiasi software di matematica, basta premere il tasto INVIO per avere la risposta immediata che si tratta di un numero primo; fra parentesi, che **questo numero è primo si sa dal 1876**!

Una curiosità: molti numeri primi hanno la forma $2^n - 1$ e sono detti **numeri di Mersenne**. I numeri primi più grandi che oggi si conoscono sono proprio due numeri di Mersenne:

- $2^{24036583} - 1$ scoperto nel Dicembre del 2003 da Michael Shaper, all'epoca uno studente di ingegneria di 26 anni, e che ha ben 6320430 cifre (la sua scrittura per esteso sarebbe lunga 20 km!)
- $2^{20996011} - 1$ scoperto da Josh Findley nel Maggio del 2004

Per ulteriori aggiornamenti puoi fare una ricerca in Internet usando come motore di ricerca la parola *Mersenne*.