ALGORITMO PER IL CALCOLO DEI NUMERI PRIMI NELLA FORMA “6n ± 1”

A cura del Gruppo Eratostene - http://www.gruppoeratostene.com/)

Con la collaborazione di Eugenio Amitrano
(http://www.atuttoportale.it/)

Contenuti dell’articolo:

↔

Introduzione

L'algoritmo proposto in questo articolo è basato sul seguente, già noto, test di primalità:

$$\frac{(p-1)!+1}{p} = k \quad se..k \in N \Rightarrow p = numero..primo$$

concentrato sulle forme aritmetiche dei primi di forma $p = 6n \pm 1$, nella quale si distribuiscono tutti i numeri primi, ad eccezione del 2 e del 3.

Descrizione dell'algoritmo

Sostituendo al numero p da testare (cioè da stabilire se è numero primo oppure no) nel test di primalità di cui sopra, la forma $p = 6n-1$, oppure $q = 6n+1$, si ottengono le forme lineari (n cresce in modo lineare da 1 ad infinito):

(1) $$k = \frac{((6n-1)-1)!+1}{6n-1} = \frac{(6n-2)!+1}{6n-1}$$

(2) $$k = \frac{((6n+1)-1)!+1}{6n+1} = \frac{(6n)!+1}{6n+1}$$

Il risultato del test dipende dalla natura di k. Se risulta k intero nella **(1)** o nella **(2)**, allora $p = 6n-1$, oppure $q = 6n+1$, è primo. Viceversa, se k è decimale, $p = 6n-1$, oppure $q = 6n+1$, è composto, quindi scartati dall'algoritmo al crescere di n.

In tale algoritmo il valore di k risulterà intero per tutti i numeri primi, ad eccezione del 2 e del 3, che non sono di forma $6n \pm 1$, mentre il valore di k risulterà intero per tutti i numeri composti.

Cosicché, applicando i due algoritmi a tutti i numeri n successivi, a partire dalla coppia di numeri 5 e 7 (i primi numeri di forma $6n \pm 1$), e scartando tutti i numeri che danno un k decimale, otteniamo la lista di tutti i numeri primi tranne il 2 e il 3.

Per verificare la primalità di questi ultimi (2 e 3), applichiamo la versione generale dell'algoritmo, cioè il test classico di Wilson. Anche per essi vale $k = 1$ intero.

$$n = 2 \quad k = \frac{(2-1)!+1}{2} = \frac{1!+1}{2} = \frac{2}{2} = 1 \quad primo \qquad n = 3 \quad k = \frac{(3-1)!+1}{3} = \frac{2!+1}{3} = \frac{3}{3} = 1 \quad primo$$

Infatti, anche 2 e 3 sono numeri primi.

Applicando il test di Wilson per gli altri valori di forma $6n\pm1$ che risultano primi dai test **(1)** e **(2)**, il valore di k risulterà intero. Infatti, l'algoritmo è stato ottenuto modificando opportunamente proprio il test di Wilson.

Ad esempio, per $p=7=6\times1+1$ e quindi con $n=1$, avremo:

Test modificato:

$$k=\frac{((6\times1+1)-1)!+1}{6\times1+1}=\frac{6!+1}{7}=\frac{720+1}{7}=\frac{721}{7}=103$$ Poiché $k=103$ è intero, 7 è primo.

Test di Wilson:

$$k=\frac{(7-1)!+1}{7}=\frac{6!+1}{7}=\frac{720+1}{7}=\frac{721}{7}=103$$ Anche con Wilson $k=103$

Con il test modificato, i primi numeri composti ad essere scartati sono $25=5\times5$ e $35=5\times7$, poiché i loro k sono decimali.

Considerazioni importanti

Programmando opportunamente i due test **(1)** e **(2)** con apposito software in linguaggio MAPLE o simili, per esempio per n fino a 100, si otterranno tutti i numeri primi fino a $6\times100\pm1$. Gli ultimi due della lista saranno 599 e 601. Ovviamente solo quei numeri con k intero, altrimenti sarebbero composti e quindi scartati dalla lista finale. In questo caso, 599 e 601 sono entrambi primi e quindi primi gemelli. (*Due numeri primi p e q, con $p<q$, si dicono gemelli se $q=p+2$*).

Insomma, quest'algoritmo potrebbe essere definibile un moderno "Crivello di Eratostene" automatizzato, e cioè una specie di "macchina" matematica, adibita alla produzione dei numeri primi, tanto sognata dai matematici. Inoltre, si concentra sui soli numeri di forma $6n\pm1$, tra i quali si annidano tutti i numeri primi maggiori di 3.

Il Crivello di Eratostene, quello classico, si applica a tutti i numeri interi, ovviamente con maggiore lentezza nel noto procedimento. Algoritmi informatizzati e quindi automatizzati che, eliminando progressivamente tutti i numeri con k decimale e quindi composti, elencano tutti i numeri primi. Il problema, già noto è che essi sono sempre più lenti al crescere di n, poiché i numeri $(6n\pm1)!$ crescono molto rapidamente. I calcoli diventano sempre più lunghi e quindi più lenti. Per questo motivo, bisognerebbe attendere computer sempre più potenti e veloci, oppure usare altri test di primalità più veloci per programmare algoritmi più rapidi di quello da noi proposto.

Riconducibilità nella forma "6n ± 1"

Prendiamo in considerazione un nostro test precedente, simile ad un antico test cinese:

Test cinese: $k = \frac{2^n}{n}$ con resto di 2 n è primo;

Nostro test: $k = \frac{2^n - 2}{n}$ con k intero se n è primo.

Questo test si imbatteva nei famosi numeri di Carmicael, per i quali il test non funzionava.

Tali numeri, fino a 10.000, sono: 341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911.

Questi numeri sono stati trovati dal *Prof. Giuseppe Guarino* con un software in linguaggio MAPLE (*in seguito compilò la lista di tali numeri fino a 100.000*).

Una conseguenza delle suddette forme $6n \pm 1$ è la spiegazione per cui i numeri di forma $n! \pm 1$ possono essere o non essere primi.

Infatti, $1 \times (2 \times 3) \times (4 \times 5 \times 6 ... \times n) \pm 1 = 6 \times (4 \times 5 \times 6 ... \times n) \pm 1 = 6n' \pm 1$. In questo secondo caso si chiamano numeri primi euclidei, (***Vedi Rif.1***), perché sono anch'essi nella forma $6n \pm 1$, proprio come tutti i numeri primi. E cosi pure per i primordiali $n\#$, seguiti da ± 1, e quindi $n\# \pm 1 : (2 \times 3) \times (5 \times 7 \times 11 \times ... \times n) \pm 1$, abbiamo la forma $6n \pm 1$.

Anche i numeri primi di Fermat e di Mersenne sono riconducibili a tale forma generale.

I numeri di Mersenne $2^p - 1$ sono riconducibili alla forma $6n \pm 1$ solo se p è dispari, e spesso è anche primo. La forma $2^p - 1$ con p pari è sempre multiplo di 3 e quindi non può mai essere primo; ad esempio $2^6 - 1 = 63 = 3 \times 21$ e cosi via per tutti i numeri p pari, con la sola eccezione di 2, poiché $2^2 - 1 = 3$ primo.

Lo stesso simile ragionamento vale anche per i numeri di Fermat, infatti, i numeri di forma: $2^{2^n} + 1$ sono riconducibili alla forma $6n \pm 1$, ad esempio $2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17 = 6 \times 3 + 1$.

Riferimenti

1) "**I numeri primi di Euclide (o Euclidei)**" – *Prof. Annarita Tulumello*.
Link: http://www.gruppoeratostene.com/articoli/Numeri%20primi%20euclidei.pdf