Crivello di Eratostene semplificato

Raffaele Cogoni

Si presenta una procedura per trovare i numeri primi, si tratta di una semplificazione del Crivello di Eratostene.

Teoremi introduttivi

Teorema 1 (Teorema di Dirichlet)
Per ogni a,b interi coprimi (con b>0) esistono infiniti numeri primi della forma a+nb con n naturale.

Corollario 1
I numeri primi della forma 6n+1 e 6n+5 sono infiniti con n naturale.

Teorema 2 (Teorema di Petrus bungus)

"...semper ... numeri primi post binarium et ternarium, in senariorum multiplicium vicinia collocati comperiuntur, aut uno minores, aut uno majores."

(tutti i numeri primi maggiori di 3 e di 2 sono vicini alla tavola moltiplicativa del 6 e sono del tipo 6n + 1 o 6n + 5

Corollario 2
Tutti i numeri primi >3 sono della forma 6n+1 e 6n+5 e sono infiniti in ciascuna progressione.

Una dimostrazione del teorema di Pietro Bongo

Data la $(*)$ 6m+1, con $m \in N$ che genera la successione 1,7,13,19,25,31, 37,43, 49,55,61 …

nella quale ho notato che compaiono i numeri primi 7,13,19, 31, 37, 43…

con ulteriori approfondimenti ho trovato che anche la $(**)$ 6m+5 con $m \in N$, genera un'altra successione: 5,11,17, 23, 29, 35, 41, 47, 53, 59, 65, 71 …

anche qui compaiono numeri primi 5,11,17,23,29,41,47,59,71… quindi mi sono chiesto se le $(*)$, $(**)$ generano oltre numeri composti, anche tutto l'insieme dei numeri primi, e in effetti ho trovato la seguente dimostrazione :

Dimostrazione

Ricordiamo preliminarmente il teorema di esistenza e unicità di quoziente e resto: dati due numeri interi n e b>0, esiste una ed una sola coppia di interi m e r tali che $a=m\cdot b+r$, con $0\leq r<b$

Pertanto, dividendo per 6 un qualsiasi numero intero n , in applicazione del teorema sopra ricordato, si ha che il resto della divisione è un numero intero r, con $0\leq r<6$. Vale a dire che ogni n fissato può essere espresso in una sola delle seguenti forme:

$a=m\cdot 6+0$

$a=m\cdot 6+1$

$a=m\cdot 6+2$

$a=m\cdot 6+3$

$a=m\cdot 6+4$

$a=m\cdot 6+5$

Sia n un numero primo. Esso allora non potrà essere espresso nelle forme:

$a=m\cdot 6+0$

$a=m\cdot 6+2$

$a=m\cdot 6+3$

$a=m\cdot 6+4$

perché, se così fosse, tale numero sarebbe composto.

Pertanto un numero primo n può essere espresso in una delle due forme seguenti:

$a=m\cdot 6+1$

$a=m\cdot 6+5$

Osserviamo ora che l'insieme $A=\{n\in Z \mid n=m\cdot 6+5, m\in Z\}$ è uguale all'insieme $B=\{n\in Z \mid n=m\cdot 6-1, m\in Z\}$.

Sia infatti $n\in A$, si ha $n=m\cdot 6+5=m\cdot 6+6-6+5=(m+1)\cdot 6-1$ e quindi $n\in B$.

Viceversa, sia $n\in B$, si ha $n=m\cdot 6-1=m\cdot 6-6+6-1=(m-1)\cdot 6+5$ e quindi $n\in A$.

In conclusione si è dimostrato che ogni numero primo n può essere espresso in una delle due forme seguenti:

- $a=m\cdot 6+1$
- $a=m\cdot 6-1$

Ho dimostrato questo teorema a ottobre del 2010, purtroppo l' illusione dell' unicità è durata solo un anno, poco tempo fa sono venuto a conoscenza della dimostrazione del 1599 di un matematico Bergamasco, Pietro Bongo.

Di seguito, svilupperò una procedura di cui sono l'autore, da me scoperta a ottobre del 2010 , è una sorta di Crivello di Eratostene semplificato, in pratica riduce il procedimento, pari a 1/3 rispetto al Crivello di Eratostene

Il crivello di Eratostene semplificato

Con le due serie sovrapposte S1 e S2,

S1 $0 \le n,\ \ n6+1$ 1,7,13,19,25 ,31,37,43,49 ,55, 61, 67, 73,79,85 ,91, 97, 103 …

Verso (a) ↑

Verso (b) ↓

S2 $0 \le n,\ \ n6+5$ 5,11,17,23,29,35, 41,47,53,59,65,71,77 , 83, 89,95 ,101,107…

si possono identificare con facilità i numeri composti (i numeri sottolineati), basta contare in un verso e nell'altro le due successioni seguendo il verso delle frecce, iniziando dal 5, quindi contare 5 sequenze 1, 7, 13, 19, <u>25</u>, poi le 5 successive 31, 37, 43, 49, <u>55</u> e cosi di seguito...

e nell'altro verso 11, 17, 23, 29, <u>35</u> le 5 successive 41, 47, 53, 59, <u>65</u>… e cosi di seguito...

stesso procedimento per il 7, quindi 1, 5, 11, 17, 23, 29, <u>35</u> poi 41, 47, 53, 59, 65, 71, <u>77</u>… e nell'altro verso 13,19, <u>25</u>, 31, 37, 43, <u>49</u>, poi 61, 67, 73, 79, <u>85</u>, <u>91</u>…

e seguendo lo stesso procedimento per i numeri primi 11, 13,17, 19…

$0 \le n,\ \ n6+1$ 1,7,13,19,<u>25</u> ,31,37,43,<u>49</u> ,<u>55</u>, 61, 67, 73,79,<u>85</u> ,<u>91</u>, 97, 103 …

↑

↓

$0 \le n,\ \ n6+5$ 5,11,17,23,29,<u>35</u>, 41,47,53,59,<u>65</u>,71,<u>77</u> , 83, 89,<u>95</u> ,101,107…

In pratica, dalle due serie sovrapposte, escludo i numeri composti (i numeri sottolineati) , ne consegue che rimane l'insieme dei numeri primi.

Vediamo come funziona il Crivello di Eratostene semplificato.

L'obiettivo del crivello è di trovare tutti i numeri composti i cui fattori primi sono > 3 (infatti tutti gli altri vengono eliminati automaticamente in quanto consideriamo solo le due progressioni qui sotto). Indichiamo con (1) la progressione 6n+1 e con (2) la progressione 6n+5 con n naturale.

(1) 1,7,13,19,25 ,31,37,43,49 ,55, 61, 67, 73,79,85 ,91, 97, 103 …

↑

↓

(2) 5,11,17,23,29,35, 41,47,53,59,65,71,77 , 83, 89,95 ,101,107…

Per ogni numero primo (p) in ciascuna delle serie, i suoi composti si trovano ogni p numeri seguendo le frecce, cioè andando avanti di p in p lungo la propria progressione e tornando indietro e salendo (o scendendo nel caso (1)) continuando a contare.

Esempio 1.

Proviamo a farlo con il numero 5.
5 è della forma 6n+5.
Continuando nella stessa progressione e eliminando ogni 5 otteniamo 11, 17, 23, 29, 35, 41, 47, 53, 59, 65, etc.
Se vogliamo eliminare i multipli di 5 nella progressione (1) allora prima torniamo indietro nella successione (2) , ma 5 è il primo numero, quindi si sale direttamente e otteniamo 1, 7, 13, 19, 25, 31, 37, 43, 49, 55, etc.

Esempio 2.

Proviamo a farlo con il numero 7.
7 è della forma 6n+1.
Continuando nella stessa progressione e eliminando ogni 7 otteniamo 13, 19, 25, 31, 37, 43, 49, 55, 61, 67, 73, 79, 85, 91, etc.
Se vogliamo eliminare i multipli di 7 nella progressione (2) allora prima torniamo indietro nella successione (1) ,(arrivati al primo iniziamo a scendere) e otteniamo 1, 5, 11, 17, 23, 29, 35, 41, 47, 53, 59, 65, 71, 77, etc.

Esempio 3.

Proviamo a farlo con il numero 11.
11 è della forma 6n+5.
Continuando nella stessa progressione e eliminando ogni 11 otteniamo 17, 23, 29, 35, 41, 47, 53, 59, 65, 71, 77, etc.
Se vogliamo eliminare i multipli di 11 nella progressione (1) allora prima torniamo indietro nella successione (2) , (arrivati al primo iniziamo a salire) e otteniamo , 5, 1, 7, 13, 19, 25, 31, 37, 43, 49, 55, etc.

Dimostrazione:
Il primo passo della dimostrazione è mostrare che, per ogni numero p primo $\neq 2, 3$, $\exists$ un multiplo di p in entrambe le progressioni . Poi dimostreremo che ogni multiplo di p su ciascuna progressione sta a "distanza" hp (con h naturale) dal primo multiplo di (1) e (2) rispettivamente; infine dimostriamo che tra il primo multiplo di p in (1) e il primo in (2) ci stanno p numeri (seguendo il percorso dell'algoritmo).
Partiamo della considerazione che, per ogni numero primo p, $(\mathbb{Z}_{P,} +, .)$ è un campo e quindi ogni suo elemento, tranne 0, ha inverso moltiplicativo (dove $0 = [0]$).
Consideriamo prima la (1).
Un numero della forma 6n+1 è multiplo di p se $6n + 1 \equiv_p 0$ e quindi, poiché esiste l'inverso di 6 mod p (6 e p coprimi in quanto p primo) e denotiamo con 6_p^{-1} il rappresentante < p, allora $n \equiv_p -6_p^{-1} \equiv_p p - 6_p^{-1}$ sse $n = p - 6_p^{-1} + hp$ con $h \in \mathbb{N}$ e questo è naturale per ogni h naturale. Perciò $\exists$ n tc $p|6n + 1$.

Con un procedimento analogo si ottiene che i numeri della forma (2) e per ogni n naturale $p|6n + 5$ sse $n = 6_p^{-1} + hp$ con h naturale.
La parte restante della dimostrazione è praticamente già fatta. Infatti le relazioni n = p $- 6_p^{-1} + hp$ e n = $6_p^{-1} + hp$ con h naturale dicono che la "distanza" tra due multipli consecutivi tra p e p. Inoltre prima di $6\left(6_p^{-1}\right) + 5$ e $6\left(p - 6_p^{-1}\right) + 1$ non ci sono altri numeri multipli nelle rispettive progressioni, altrimenti le due congruenze sarebbero verificate in $\mathbb{N}$ per valori di h negativi, ma ciò è assurdo in quanto 6_p^{-1} è il minimo rappresentante degli inversi di 6 mod p ed è quindi < p, perciò anche per solo h = -1 si ha che n < 0.
Infine si vede che tra il primo multiplo di p in (1) e il primo in (2) ci stanno p numeri (seguendo il percorso dell'algoritmo) perché i primi multipli delle progressioni sono per n = 6_p^{-1} e n = p $- 6_p^{-1}$, quindi ci sono numeri con n da 0 a 6_p^{-1} prima di 6_p^{-1} , cioè 6_p^{-1} numeri e ugualmente ci sono p $- 6_p^{-1}$ numeri prima del primo multiplo nella progressione (1), quindi in totale ci sono 6_p^{-1} + p $- 6_p^{-1}$ = p numeri.

Cagliari 23/05/2014