

Nota correttiva per la Storia di Sophie-Germain

L Ing. Rosario Turco segnala una precisazione matematica nella storia di Sophie - Germain , che riportiamo testualmente, per i visitatori eventualmente interessat i ai numeri primi della grande matematica francese.

Se $p = 4k+1$ e numero primo allora $M_p = 2^{p-1}$ non è numero primo, non è vera.

I contro-esempi:

$$4 \cdot 1 + 1 = 5 \text{ primo}$$

$$2^5 - 1 = 31 \text{ primo}$$

$$4 \cdot 2 + 1 = 9 \text{ non primo}$$

$$4 \cdot 3 + 1 = 13 \text{ primo}$$

$$2^{13} - 1 = 8191 \text{ primo}$$

p può essere di sia di forma $4k+1$ che $4k+3$.

Mentre nei numeri di Sophie Germain

$$S = 2p + 1$$

Sia S che p numeri primi e p può essere di forma $4k + 1$ o $4k + 3$

$$p = 2 \quad S = 5$$

$$p = 3 \quad S = 7$$

$$p = 5 \quad S = 11$$

$$p = 11 \quad S = 23$$

Se $p = 4k - 1$ con $k > 1$, allora in alcuni casi $M_p = 2^{p-1}$ è composto

$$\text{Es: } 11 = 4k - 1 = 4 \cdot 3 - 1 = 2^5 + 1$$

$$k > 1 \text{ perché } k = 1 \quad p = 3 \text{ e } 2^3 - 1 = 7$$

ma anche così non è sempre vero

Es.:

$$4 \cdot 2 - 1 = 7 \text{ e } 2^7 - 1 = 127$$

$$4 \cdot 5$$

$$- 1 = 19 \text{ primo}$$

Tutto questo è importante per i test di primalità. Vedi articolo [TECNICHE DI PRIMALITÀ](#).

Teorema sui Numeri primi di Sophie Germain

I numeri primi di **Sophie Germain** sono tali che:

$$S = 2p+1$$

con p e S contemporaneamente primi ed S è di forma $4n-1$.

Dimostrazione

Ora se $S=4n-1=2p+1$ con p numero primo allora $4n=2p+2=2(p+1)$ e quindi $2n-1=p$ ovvero otteniamo un dispari che è un primo. Esiste una connessione tra numeri di Sophie Germain e numeri di Mersenne.

Teorema sui Numeri primi di Mersenne (R. Turco)

Se $p = 4k-1$ numero primo con $k>0$ e $k \not\equiv 0 \pmod{3}$ e $2p+1$ è primo allora $M_p=2^{p-1}$ non è primo .

Lo stesso Teorema precedente si può riesprimere nel seguente modo:

Teorema equivalente sui Numeri primi di Mersenne (R. Turco)

Se $p = 4k-1$ numero primo allora M_p è composto se sono contemporaneamente vere tre condizioni:

- 2^{p+1} numero primo
- $(p+1) \bmod 4 = 0$
- $((p+1)/4) \bmod 3 = 0$

Esempi:

$p=11=4*3-1$ $k=3*1$ $M_p=2^{11}-1$ non primo

$p=23=4*6-1$ $k=3*2$ $M_p=2^{23}-1$ non primo

$p=47=4*12-1$ $k=3*4$ $M_p=2^{47}-1$ non primo

Teorema sui numeri primi di Wagstaff ed i numeri primi di Mersenne (R. Turco)

Se $W = (4k+5)/3$ è un intero dispari con $k > 1$ e $W > 3$, se W è un numero primo di Wagstaff tale che $(2^p+1)/3$ con p primo, allora k è un numero primo di Mersenne anche esso.

Dimostrazione

Un numero primo di Wagstaff è per definizione un numero primo con $W = (2^p+1)/3$ dove p è un numero primo.

Se $p=4k-1$ con $k > 0$ e k multiplo di 3 con 2^{p+1} primo allora W non è primo e non intero.

Ipotizziamo W numero primo. Se $M_p=2^p-1$ allora $3W=M_p+2$.

Sappiamo che $M_p=4k+3$ per cui $3W=4k+5$ da cui $W = (4k+5)/3$.

Ora per essere W intero deve essere $k > 0$. Con $k=1$ $W=3$ è primo ma $k=1$ non è un numero primo di Mersenne. Il successivo k , per avere W intero e numero primo, è $k=7$ che è un numero primo di Mersenne (per cui $k > 1$ per avere i numeri primi di Mersenne e $W > 3$). Per cui a questo punto per ogni numero primo W di Wagstaff abbiamo un numero primo di Mersenne M_p .

Questa tecnica non crea però tutti i numeri primi di Mersenne, difatti salta 3 e 5.

Il Teorema, di fatto, ha bisogno di 2 condizioni affinché M_p sia primo: p numero primo e di un certo tipo W numero primo. Ovviamente i numeri primi sono sia di forma $4k-1$ e $4k+3$.

Teorema equivalente sui numeri primi di Wagstaff ed i numeri primi di Mersenne

Se p è un numero primo, che nel caso $p=4k-1$ abbia $k > 1$ e non multiplo di 3, se $W = (2^p+1)/3$ è un numero primo di Wagstaff, allora M_p è un numero primo di Mersenne.

Nuova Conggettura di Mersenne

La congettura afferma che:

Per ogni numero naturale dispari p , se almeno due delle seguenti affermazioni sono vere, allora lo sarà anche la terza:

- $p = 2^k \pm 1$ o $p = 4^k \pm 3$ per un qualche k naturale.
- $2^p - 1$ è primo (Numero primo di Mersenne)
- $(2^p + 1) / 3$ è primo (Numero primo di Wagstaff).

Se p è un numero dispari composto, allora, anche $2^p - 1$ e $(2^p+1)/3$ lo sono. Questa è

L'unica condizione necessaria per testare valori primi (test di primalità) che soddisfino la congettura.

Renaud Lifchitz ha dimostrato che la nuova congettura di Mersenne è vera fino a 12,441,900 testando sistematicamente tutti i numeri primi per cui è noto che vale almeno una delle condizioni (vedi <http://www.primenumbers.net/rl/nmc/>).

La Nuova Congettura di Mersenne è in linea con i con quanto visto prima.

Dimostrazione Nuova Congettura di Mersenne (R. Turco)

Servono almeno due condizioni come dice l'enunciato della congettura.

Dal Teorema equivalente sui numeri primi di Wagstaff ed i numeri primi di Mersenne abbiamo visto che serve innanzitutto che i primi p di tipo $4k + 1$ siano con $k > 1$ e con k non multiplo di 3. Numeri primi p che possono essere di forma $4k + 1$ e rispettare tale condizione sono quelli ad esempio $2^{2k} + 1$.

Ad esempio:

$$2^2 + 1 = 4 \cdot 1 + 1 = 5$$

$$2^4 + 1 = 4 \cdot 4 + 1 = 17$$

$$2^8 + 1 = 4 \cdot 64 + 1 = 257$$

Tuttavia non esistono solo i numeri primi di forma $4k + 1$, anzi per coprire tutto l'insieme P dei numeri primi occorre considerare anche i numeri primi di forma $4k + 3$; ma analogamente i primi $4k + 3$ sono di tipo $4k + 3$; alcuni esempi sono:

$$4^1 + 3 = 4 \cdot 1 + 3 = 7$$

$$4^2 + 3 = 4 \cdot 4 + 3 = 19$$

$$4^3 + 3 = 67$$

Anche dai Teoremi precedenti era che se $W = (2^{p+1})/3$ è un numero primo di Wagstaff allora M_p è un numero primo di Mersenne.

La parte sfruttabile di questa congettura in ambito FPMG è che se p è primo, si può valutare la primalità di M_p , attraverso un numero più piccolo di M_p , ovvero con i numeri primi di Wagstaff!

This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.