Riconducibilità dei numeri primi di Fermat e Mersenne 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:

↔

Enunciato

I numeri di Mersenne $M = 2^p - 1$ e di Fermat $F = 2^{2^n} + 1$, se primi, sono riconducibili alla forma generale dei numeri primi $6n \pm 1$, ma non viceversa.

Dimostrazione

Il matematico francese P. Martin Mersenne (1588 – 1648) si accorse che alcuni numeri della forma $2^p - 1$ con p primo, erano primi:

(1) $M = 2^p - 1$

Qualsiasi numero primo maggiore di 3 è sempre riconducibile alla forma $6n \pm 1$. Presi due numeri primi, $p = 6n \pm 1$ e $q = 6m + 1$ con $m > n$, possiamo scrivere la **(1)** nella seguente forma:

(2) $2^{6n \pm 1} - 1 = 6m + 1$

Attraverso opportuni calcoli, possiamo associare ad ogni valore di n, 2 diversi valori di m, svolgendo la **(2)** come un'equazione di primo grado con incognita m:

$$m' = \frac{2^{6n-1} - 2}{6} \qquad m'' = \frac{2^{6n \pm 1} - 2}{6}$$

Da qui poi ricavare due possibili numeri primi per ogni n: $Mp' = 6m - 1$ e $Mp'' = 6m + 1$, che noi definiremo primo e secondo numero di Mersenne.

Esempi:

Per $n = 1$

Numeri di Mersenne:

$p' = 2^{6 \times 1 - 1} - 1 = 2^5 - 1 = 32 - 1 = 31$ $\qquad$ $p'' = 2^{6 \times 1 + 1} - 1 = 2^7 - 1 = 128 - 1 = 127$

Valori di m:

$m' = \frac{2^5 - 2}{6} = \frac{32 - 2}{6} = \frac{30}{6} = 5$ $\qquad$ $m'' = \frac{2^7 - 2}{6} = \frac{128 - 2}{6} = \frac{126}{6} = 21$

Numeri di Mersenne da m:

$Mp' = 6m' + 1 = 6 \times 5 + 1 = 31$ $\qquad$ $Mp' = 6m'' + 1 = 6 \times 21 + 1 = 127$

Per $n=2$

Numeri di Mersenne:

$p'=2^{6\times 2-1}-1=2^{11}-1=2048-1=2047$ $\qquad$ $p''=2^{6\times 2+1}-1=2^{13}-1=8192-1=8191$

Valori di m:

$m'=\frac{2^{11}-2}{6}=\frac{2048-2}{6}=\frac{2046}{6}=341$ $\qquad$ $m''=\frac{2^{13}-2}{6}=\frac{8192-2}{6}=\frac{8190}{6}=1365$

Numeri di Mersenne da m:

$Mp'=6m'+1=6\times 341+1=2047$ $\qquad$ $Mp'=6m''+1=6\times 1365+1=8191$

In sintesi, per ogni n e per ogni $p=6n\pm 1$, si hanno $P=2^{6n\pm 1}-1=6m+1$, due diversi numeri di Mersenne, dei quali nessuno, uno o entrambi (coppie di primi gemelli) possono essere primi.

Così pure per ogni numero $F=2^{2^n}+1$ di Fermat:

$$2^{2^n}+1=6m-1$$

Numeri di Fermat: sono numeri di forma generale $2^{2^n}+1$, in base alle forme $6n\pm 1$, sono sempre divisibili per 6 (poiché 2^{2^n} è di forma $6m-2$), per cui $2^{2^n}+1$ risulta di forma $6m-1$ (ricade sempre nella colonna delle forme $6m-1$), cosicché anche $2^{2^n}+1$ ricade sempre in tale colonna, che contiene soltanto primi e prodotti tra primi (come pure la colonna $6m+1=6m-1+2$.

Per esempio per 2^n pari: $2^2=4=6\times 1-2$, se aggiungiamo 1 otteniamo, $6\times 1-1=6-1=5$, e $2^{2^2}=2^4=16=6\times 3-2$, se aggiungiamo 1 abbiamo $6\times 3-1=17$, numero primo di Fermat.

<u>Tabella 1</u>

n	***F=6m-2***	***F+1***	***6m-1***	***6m***	***6m+1***
1	4	5	**5**	6=6×1	7
2	16	17	**17**	18=6×3	19
3	256	257	**257**	258=6×43	259
4	65536	65537	**65537**	25538=6×10923	65539
…	…	…	**…**	…	…

E questi sono i primi quattro numeri primi di Fermat attualmente conosciuti.
(*Vedi alla voce di Wikipedia: “**Numero di Fermat**”*)

Con una tabella simile, si hanno i numeri di Mersenne, di forma 2^n con n dispari, (tranne il 2 iniziale) di forma $6m+1$ (*in questa tabella appare solo il 7*):

Tabella 2

n	*2^n=6m+2*	*(2^n-1)*	*6m-1*	*6m*	*6m+1*
2	4	3	1	2	**3 (irregolare)**
3	8=6×1+2	7	5	6	**7**
5	32=6×5+2	31	29	30	**31**
7	128=6×21+2	127	125	126	**127**
…	…	…	…	…	**…**

(*Vedi alla voce di Wikipedia: "**Numero di Mersenne**"*)

Numeri palindromi

Per i numeri primi palindromi, ossia leggibili da destra a sinistra e viceversa senza variazione di valore, come per tutti i primi, sono riconducibili della forma $6n\pm1$.

Ad esempio il numero 353, che è un palindromo abbiamo $353=6*59-1$.

I numeri palindromi formati dalle stesse cifre, per essere primi possono contenere solo la cifra 1, ad esempio 11111, poiché se fossero formate da 3, 5 o 7 sarebbero multipli della cifra base, e quindi non primi. Se fossero tutti 9, invece, sarebbero multipli anche di 3. Pertanto rimane l'unica possibilità che il numero primo palindromo sia fatto solo da cifre 1. Inoltre, molti numeri palindromi di questo tipo non sono primi, bensì composti:

Tabella 3

n cifre	*Numero palindromo*	*Test*	*6m±1*
2	11	Primo	6×2-1
3	111	Composto, multiplo di 3	
4	1111	Composto, 101×11	6×185+1
5	11111	Composto, 41×271	6×1582-1
6	111111	Composto, multiplo di 3	
7	1111111	Composto	6×185185+1
8	11111111	Composto	6×1851852-1
9	111111111	Composto, multiplo di 3	

Fino ad oggi si conoscono solo 5 numeri primi palindromi formati dalle sole cifre 1, e sono quelli con 2, 19, 23, 317 e 1031 cifre.

Ci sono altri numeri primi palindromi, ne esistono 15 di tre cifre, e tra essi sussiste una curiosa identità: 101 + 131 + 151 = 383, e tutti primi palindromi.

Riferimenti

Rubrica "**Che numeri – I mattoni dell'aritmetica**" di ***Silvana Leggerini***, rivista Newton n.1/2001.