Alessandra Di Berardino
Relatore: Prof. Andrea Loi

Università degli studi di Cagliari

Facoltà di Scienze Matematiche Fisiche e Naturali

I NUMERI DI FERMAT SONO ASOCIALI

Tesi di Alessandra Di Berardino

24 Luglio 2015

Introduzione

Fermat (1601-1665) divenne noto per i suoi Teoremi: il piccolo Teorema di Fermat , l'ultimo Teorema di Fermat, ma anche per una congettura :

Congettura

Tutti i numeri di questa forma

$$F_m = 2^{2^m} + 1 \quad \textit{per m=0,1,...}$$

sono primi.

I primi 5 numeri della sequenza sono primi:

$$F_0 = 3 \quad F_1 = 5 \quad F_2 = 17 \quad F_3 = 257 \quad F_4 = 65537$$

Le Scoperte

Nel 1732 Eulero dimostrò che Fermat si sbagliava dando la fattorizzazione del numero F_5:

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$$

Fino al 1796 i numeri di Fermat rimasero una curiosità matematica, per via delle insormontabili difficoltà del calcolo diretto e per via dell'utilizzo di metodi della teoria dei numeri ogni volta sempre più complicati.

Le Scoperte

L'interesse di questi numeri aumentò quando Gauss (1777-1855) trovò un teorema che esprimesse un interessante legame tra la costruzione dei poligoni regolari di Euclide e i numeri primi di Fermat. Gauss dimostrò che si può costruire con riga e compasso un poligono regolare con n lati se e solo se n è il prodotto di una potenza di 2 per un prodotto finito di numeri di Fermat primi e distinti.

Le Scoperte

A tutt'oggi non si è ancora riusciti a dimostrare se esistono altri numeri primi oltre ai numeri F_m per $m \leqslant 4$. Attraverso l'uso dei computer si è riusciti a trovare che F_m per $5 \leqslant m \leqslant 30$ sono composti, ma già per $m = 31$ non si è ancora arrivati a una conclusione.

Le Domande

Da qui iniziarono le numerose domande sui numeri di Fermat a cui non si è data ancora una risposta:

- ci sono altri numeri di Fermat che sono numeri primi?
- questi primi sono un numero finito?

Applicazioni pratiche

I numeri di Fermat hanno anche diverse applicazioni pratiche:

1. possono essere utilizzati per l'elaborazione del segnale digitale;
2. possono essere usati per moltiplicare velocemente dei grandi numeri binari;
3. vengono usati nell'analisi dell'equazione logistica che descrive il Caos.

Definizioni principali

Definizione

Indichiamo con $\sigma(n)$ quella funzione che associa ad ogni numero intero n la somma dei suoi divisori positivi.

Definizione

Un numero perfetto è un intero positivo n tale che:

$$\sigma(n) = 2n$$

Definizione

Due numeri interi positivi m e n sono chiamati Amici se :

$$\sigma(m) = \sigma(n) = m + n$$

I numeri di Fermat sono asociali

Tesi di laurea in Matematica

Alessandra Di Berardino
Relatore: Prof. Andrea Loi

Teorema (I numeri di Fermat sono asociali)

Un numero di Fermat non è mai perfetto o parte di una coppia di amici, cioè un numero di Fermat F_m è tale che

$$\sigma(F_m) \neq 2F_m$$

e non esiste un intero positivo x con $x \neq F_m$ tale che

$$\sigma(x) = \sigma(F_m) = x + F_m.$$

Strumenti utili per il teorema

Tesi di laurea in Matematica

Alessandra Di Berardino
Relatore: Prof. Andrea Loi

Proposizione (Rosser - Schoenfeld)

$$\sigma(y) < \left(1.8 \log\log y + \frac{2.6}{\log\log y}\right) y \qquad \textit{per tutti gli } y \geqslant 3$$

Definizione

La funzione di Eulero è quella funzione che associa a un numero intero m il numero degli interi più piccoli di m e primi con esso. Se scrivo la decomposizione in fattori primi di m, cioè :

$$m = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$$

La funzione di Eulero è

$$\varphi(m) = \prod_{i=1,\cdots,s} p_i^{r_i - 1}(p_i - 1)$$

Il Teorema di Lucas

Nel 1878, Èdouard A. Lucas stabilì un criterio relativo alla forma generale dei divisori primi dei numeri di Fermat, ossia ogni divisore primo p di F_m , $m > 1$, soddisfa la congruenza

$$p \equiv 1 \pmod{2^{m+2}}$$

che può essere espressa come segue:

Teorema (Lucas)

Se $m > 1$ e p è un numero primo tale che $p|F_m$, allora p è della forma

$$p = k2^{m+2} + 1$$

dove k è un numero naturale.

I numeri di Fermat sono asociali

Tesi di laurea in Matematica

Alessandra Di Berardino
Relatore: Prof. Andrea Loi

Teorema (I numeri di Fermat sono asociali)

Un numero di Fermat non è mai perfetto o parte di una coppia di amici, cioè un numero di Fermat F_m è tale che

$$\sigma(F_m) \neq 2F_m$$

e non esiste un intero positivo x con $x \neq F_m$ tale che

$$\sigma(x) = \sigma(F_m) = x + F_m.$$

Dimostrazione

Supponiamo per assurdo che esista x un numero intero positivo diverso da F_m tale che

$$\sigma(x) = \sigma(F_m) = x + F_m$$

Per $m < 5$ abbiamo che i numeri di Fermat sono primi, di conseguenza l'equazione

$$\sigma(F_m) = x + F_m$$

non ammette soluzione.

Dimostrazione

Adesso supponiamo che $m \geqslant 5$.
Dato che $x \geqslant 1$ segue che

$$x^2 \geqslant \sigma(x) > F_m \geqslant F_5 > 2^{2^5}$$

in particolare $x^2 > 2^{2^5} \Rightarrow x \geqslant F_4$.
Scriviamo

$$F_m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

dove $p_1 < p_2 < \ldots < p_k$ sono numeri primi.

Dimostrazione

Dal Teorema di Lucas abbiamo che

$$\log F_m = \sum_{i=1}^{k} \alpha_i \log p_i \geqslant k \log p_1 \geqslant k \log \left(2^{m+2}+1\right)$$

usando

$$\frac{\log (y+1)}{\log (z+1)} < \frac{\log y}{\log z} \qquad \text{per tutti gli} \qquad y \geqslant z > 1$$

si ottiene

$$k \leqslant \frac{\log \left(2^{2^m}+1\right)}{\log \left(2^{m+2}+1\right)} \leqslant \frac{\log \left(2^{2^m}\right)}{\log \left(2^{m+2}\right)} = \frac{2^m}{m+2}$$

Dimostrazione

Ne segue che $\left(\sigma\left(F_m\right)=x+F_m, \dfrac{\sigma\left(y\right)}{y} \leqslant \dfrac{y}{\varphi\left(y\right)}, y \geqslant 1\right)$

$$1+\frac{x}{F_m}=\frac{\sigma\left(F_m\right)}{F_m} \leqslant \frac{F_m}{\varphi\left(F_m\right)}=\prod_{i=1}^{k}\left(1+\frac{1}{p_i-1}\right)$$

applico il logaritmo:

$$\log\left(1+\frac{x}{F_m}\right)<\sum_{i=1}^{k}\frac{1}{p_i-1}$$

Dimostrazione

Dal Teorema di Lucas otteniamo che

$$\log\left(1+\frac{x}{F_m}\right) < \frac{m\log 2}{2^{m+2}}$$

Ne consegue che

$$x < F_m$$

Dimostrazione

Dato che

$$\log(1+y) > \frac{y}{2} \quad \text{per tutti gli } y \in (0,1)$$

ne consegue che

$$\frac{x}{2F_m} < \frac{m \log 2}{2^{m+2}}$$

Allora

$$x < \frac{F_m m \log 2}{2^{m+1}}$$

Dimostrazione

Usiamo la proposizione di Rosser-Schoenfeld

$$x + F_m = \sigma(x) < \left(1.8 \log\log(x) + \frac{2.6}{\log\log(x)}\right) x$$

Dal momento che $x \geqslant F_4$, segue che

$$\log\log(x) > 1.$$

Quindi

$$F_m < 4.4 \frac{F_m m \log 2}{2^{m+1}} \log\log F_m$$

cioè

$$2^{m+1} < 4.4 m \log 2 \log\log F_m.$$

Tuttavia $F_m = 2^{2^m} + 1$

$$F_m < 2^{2^{m+1}}$$

Dimostrazione

quindi

$$2^{m+1} < 4.4m \log 2 \left((m+1)\log 2 + \log\log 2\right).$$

Ma questa disuguaglianza è impossibile in quanto
la parte a sinistra è più grande della parte che sta a destra
per tutti gli

$$m \geqslant 5.$$

Il teorema resta così dimostrato.

Fine

Grazie per l'attenzione