

Storia di Pierre de Fermat



Pierre de Fermat

Pierre de Fermat nacque a Beaumont-de-Lomagne il 17 agosto 1601 e morì a Castres (Tarn) il 12 gennaio 1665), è stato un matematico francese che ha dato importanti contributi allo sviluppo della matematica moderna.

“Studiò legge, e divenne avvocato al Parlamento, di Tolosa dove si trasferì nel 1631. Nello stesso anno sposò Luisa de Long, cugina materna dalla quale ebbe cinque figli: lavorava duramente e scrupolosamente ma nonostante ciò nel tempo libero si occupava di letteratura (compose persino alcuni versi), e soprattutto di matematica. Per questo Fermat è stato chiamato “Il principe dei dilettanti”... Nel 1648 divenne Consigliere del Re al Parlamento di Tolosa e mantenne tale carica per i successivi 17 anni. Morì nel 1665 a Castres, città a 79 chilometri (49 miglia) ad est di Tolosa...”

“In particolare, è stato il precursore del calcolo differenziale con il suo metodo per la individuazione dei massimi e dei minimi delle funzioni, analogo a quello del calcolo differenziale che sarà sviluppato da Gottfried Leibniz e Isaac Newton. Forse ancor più importanti sono le sue brillanti ricerche nella teoria dei numeri che fanno di lui il fondatore della teoria moderna. Inoltre ha dato notevoli contributi alla geometria analitica e alla probabilità...”

Fermat è famoso per la sua ipotesi, anche nota come ultimo teorema di Fermat, che è rimasta indimostrata per più di 300 anni fino al 1994; la dimostrazione è opera di Andrew Wiles...

Il campo in cui Fermat fu più attivo è sicuramente la teoria dei numeri; si può infatti considerare uno dei fondatori di questa disciplina. Espresse molte delle sue scoperte sotto forma di congettura, senza provvedere ad una dimostrazione, molte di queste furono trovate nel XVIII secolo da Eulero, mentre per altre (ad esempio il noto ultimo teorema di Fermat), si dovrà aspettare ancora oltre.

Fermat trovò che la formula $F_n = 2^{2^n} + 1$, per valori di n uguali a 1,2,3,4 dà numeri primi. Congetturò quindi che essa restituisse solo numeri primi, ma, come scoperto da Eulero, se si immette 5 nella formula essa dà come risultato un numero composto. Quando un numero che può essere scritto in questa forma è primo viene chiamato numero primo di Fermat. I numeri primi di Fermat hanno grande importanza in matematica: nel 1776 per esempio Gauss dimostrò che ogni poligono regolare costruibile con riga e compasso ha un numero di lati che è il prodotto di uno o più numeri primi di Fermat.

Fermat congetturò poi che ogni numero primo nella forma $4n+1$ può essere espresso come somma di due quadrati. Per la dimostrazione di questa congettura bisognerà aspettare Eulero. Il risultato è noto come teorema di Fermat sulle somme di due quadrati. Studiò l'equazione di Pell congetturò il teorema secondo il quale ogni numero può essere scritto come somma, al più di n numeri poligonali di grado n (tre numeri triangolari, quattro quadrati...)

Fermat scoprì senza dimostrare anche il piccolo teorema di Fermat il quale afferma che

$$a^p \equiv a \pmod{p}$$

(in altre parole che un qualsiasi numero a elevato ad una potenza prima p da resto a se diviso per p). La dimostrazione di questo teorema è dovuta anch'essa a Eulero che la generalizzò con il teorema di Eulero. Al giorno d'oggi esso è alla base dei sistemi di crittografia a base pubblica come l'RSA.

Ideò anche un nuovo test algoritmo di fattorizzazione, il cosiddetto test di Fermat

(detto anche algoritmo di Fermat, da noi riscoperto

autonomamente qualche anno fa, in seguito a ricerche sulla congettura di Goldbach e passando dalle coppie di Goldbach per la somma ($p + q = N$ pari a prodotti di Goldbach

$p \cdot q = N$, e in tali prodotti sono coinvolte la semidifferenza d dei due numeri primi p e q e la loro semisomma s , da qui il legame con Goldbach:

$$N + d = s^2, \quad (1)$$

a cui poi si ricava $p = s - d$ e $q = s + d$ (2)

L'algoritmo di Fermat consiste nel trovare efficientemente s con la formula

$$s = \sqrt{N + d} \quad \text{con } d \text{ a cominciare da } 1, \text{ per}$$

successivi tentativi: quando il secondo membro è un quadrato

perfetto, si ottengono s e d , da cui poi si ricavano p e q con le

(2). (N.d.A.A.)

“Ma il teorema più famoso di Fermat è senza dubbio, l'ultimo teorema di Fermat, Il suo enunciato è molto semplice ma dimostrarlo ha rappresentato una sfida per secoli: Esso dice infatti che non è possibile trovare quattro numeri interi x, y, z e n con $n > 2$ per cui

$$x^n + y^n = z^n$$

... (Dalla voce “Pierre de Fermat”, Wikipedia)

I nostri contributi.

Sui teoremi di Fermat abbiamo scritto i seguenti lavori, pubblicati sui nostri siti:

“Note sulle connessioni tra i numeri di Fermat, i numeri primi di Mersenne e i numeri di Collatz” , Gruppo Eratostene, anche sul database SOLAR del CNR, 2008.

“Legame tra ultimo teorema di Fermat, Zeta di Riemann e congettura di Goldbach” Ing. Rosario Turco, prof. Maria Colonnese.

“L’algoritmo di Fermat”, Gruppo Eratostene

Gruppo Eratostene