di Piergiorgio Odifreddi

professore ordinario di logica matematica all'Università di Torino
e *visiting professor* alla Cornell University di Ithaca (New York)

Una donna contro Fermat

La matematica francese Sophie Germain cercò di risolvere almeno parzialmente il teorema di Fermat

Millenni prima di Pitagora, Egizi e Babilonesi conoscevano già quelle che in seguito vennero appunto chiamate terne pitagoriche: cioè, le terne di numeri in cui la somma dei quadrati dei primi due (corrispondenti ai cateti di un triangolo rettangolo) è uguale al quadrato del terzo (corrispondente all'ipotenusa).

L'esempio più noto e antico è dato dai numeri 3, 4 e 5, che esibiscono le tre proprietà caratteristiche dei numeri costituenti le terne pitagoriche: in ciascuna deve infatti esserci un numero divisibile per 3, uno divisibile per 4 e uno divisibile per 5, anche se non sempre capita che ad avere queste proprietà siano tre numeri distinti, come invece accade nell'esempio citato.

Estrarre l'essenziale

Nel 1825, Sophie Germain cercò di generalizzare queste proprietà a somme di potenze maggiori dei quadrati, nel tentativo di risolvere almeno parzialmente il famoso teorema di Fermat: l'affermazione, cioè, che non esistono terne di numeri in cui la somma dei cubi dei primi due è uguale al cubo del terzo, e analogamente per le quarte potenze, le quinte potenze, e così via.

Cercando di estrarre l'essenziale dall'esempio precedente, la matematica francese notò anzitutto che l'esponente 2 usato nelle terne pitagoriche è un numero primo: decise dunque di restringere la propria attenzione alle potenze prime. Una restrizione comunque non riduttiva, perché Fermat stesso aveva dimostrato il caso delle quarte potenze, e ogni potenza maggiore di 2 è divisibile per 4 o per un numero primo (o entrambi).

La Germain notò inoltre che 5 è un numero primo «parente» di 2, nel senso che è il successore del suo doppio. Le venne in mente allora di definire quelli che oggi si chiamano «numeri primi di Germain», come quei numeri primi che hanno appunto un tale parente primo. Detto altrimenti, p è un primo di Germain se sono primi sia p che $2p+1$.

Di tali numeri primi ce ne sono parecchi, a partire da 2, 3, 5, 11, 23, 29, 41, 53, 83 e 89, ma non ce ne sono troppi. Per esempio, di numeri primi minori di 100 ce ne sono 25, ma solo i 10 appena enumerati sono primi di Germain. E in generale i numeri primi decrescono come il logaritmo, mentre i numeri primi di Germain decrescono come il quadrato del logaritmo.

Il teorema che Germain dimostrò nel 1825 fu che, come in ogni terna pitagorica di quadrati devono esserci un numero divisibile per 4 e uno per 5, così in ogni analoga terna di potenze di un primo di Germain devono esserci un numero divisibile per p^2 e uno per $2p+1$.

Per applicare il risultato al teorema di Fermat, servivano due passi ulteriori: generalizzare la parentela di un numero primo da uno a più parenti con proprietà analoghe a quelle sopra, e dimostrare almeno per qualche numero primo p l'esistenza di infiniti suoi parenti. Allora, almeno uno dei numeri di una terna di potenze di p avrebbe dovuto avere infiniti divisori, e questa contraddizione avrebbe dimostrato il teorema di Fermat per l'esponente p.

La prima vera matematica

Leonard Dickson dimostrò nel 1909 che non esistono numeri primi che hanno un'infinità di parenti, dunque non si può dimostrare nessun caso particolare del teorema di Fermat alla maniera di Germain. Ma mostrò che era possibile un attacco in grande al problema, e iniziò un percorso che sarebbe sfociato nella dimostrazione di Andrew Wiles nel 1995.

Il teorema di Fermat rende vuoto il teorema di Germain, ma il suo lavoro non è andato perduto. Oggi i suoi primi sono infatti diventati uno strumento fondamentale per la crittografia, e ne discute addirittura Gwyneth Paltrow nel film *Proof* (2005), in un ruolo in parte ispirato a quella che fu la prima vera matematica della storia.