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

Un teorema natalizio

Uno dei risultati più importanti di Fermat è chiamato teorema di Natale

Il 25 dicembre 1640 Pierre de Fermat (quello del famoso «ultimo teorema» che porta il suo nome) scrisse una lettera a padre Marin Mersenne (quello dei famosi numeri primi che portano il suo nome), e annunciò la dimostrazione di un risultato che, da allora, viene appunto chiamato teorema di Natale. Ma prima di enunciarlo dobbiamo fare un passo indietro, e meditare sui possibili «modi di essere» dei numeri primi.

A parte il 2, di cui non ci interesseremo, si inizia notando che alcuni primi hanno l'interessante proprietà di essere uguali alla somma di due quadrati: per esempio, 5 è 1 più 4, 13 è 4 più 9, 17 è 1 più 16, eccetera. E altri invece no: per esempio, il 3, il 7 e l'11. Nella ricerca di una regolarità, si continua osservando che i primi di un tipo si alternano, fra i numeri dispari, ai primi dell'altro tipo: detto altrimenti, i primi uguali alla somma di due quadrati sono tutti della forma $4n + 1$, e gli altri della forma $4n + 3$.

Nel 1632 Albert Girard congetturò che la cosa valesse in generale: cioè, che i numeri primi dispari uguali alla somma di due quadrati fossero esattamente quelli del tipo $4n + 1$. Una direzione era ovvia, perché ogni quadrato è del tipo $4n$ (se pari) o $4n + 1$ (se dispari): dunque, ogni somma di quadrati è del tipo $4n$, $4n + 1$ o $4n + 2$, e se è dispari l'unica possibilità è che sia del tipo $4n + 1$.

Nella sua lettera natalizia Fermat affermò di aver dimostrato anche l'altra direzione: cioè, che ogni numero primo del tipo $4n + 1$ è uguale alla somma di due quadrati. Ma la sua dimostrazione non si trovò da nessuna parte, e il primo ad averne scritta una fu Eulero nel 1749, in una lettera a Goldbach (quello della famosa congettura che porta il suo nome). In seguito se ne sono trovate molte altre, ma nessuna così elementare da stare in questa pagina.

Non solo quadrati. Ritratto del francese Pierre de Fermat, uno dei matematici più importanti del XVII secolo.

La proprietà che divide i due tipi di numeri primi si ispira ovviamente al teorema di Pitagora, perché la radice $\sqrt{p}$ di un numero p uguale alla somma di due quadrati m^2 e n^2 è ovviamente la lunghezza dell'ipotenusa di un triangolo rettangolo, che ha cateti di lunghezza m e n. In questo caso lo stesso numero p è la lunghezza dell'ipotenusa di un triangolo rettangolo, che ha cateti di lunghezza $m^2 - n^2$ e $2mn$. Per esempio, nel caso di 5, il primo triangolo ha cateti 1 e 2 e ipotenusa $\sqrt{5}$, e il secondo cateti 3 e 4 e ipotenusa 5.

Per questo motivo Diofanto chiamava «pitagorici» i primi uguali alla somma di due quadrati, che il teorema di Natale caratterizza come i primi della forma $4n + 1$. Nelle *Disquisitiones Arithmeticae* del 1801 Gauss andò oltre, dimostrando che i primi pitagorici sono l'ipotenusa di un solo triangolo rettangolo a lati interi: per esempio, 3 e 4 nel caso di 5. Ma i loro quadrati lo sono in due modi: per esempio, 7 e 24, o 15 e 20, nel caso di 25. I loro cubi, in tre modi, e così via.

La dicotomia fra primi pitagorici e non pitagorici si è in seguito rivelata fondamentale in teoria dei numeri, attraverso la connessione con i numeri interi complessi, della forma $m \pm n$. Le somme di quadrati sono infatti le norme di tali numeri, e un primo della forma $m^2 + n^2$ si può in realtà scomporre nel prodotto dei due interi complessi $m + in$ e $m - in$. Cioè, i primi pitagorici sembrano primi se li si guarda dal ristretto punto di vista dei numeri interi reali, ma si rivelano non esserlo quando li si osserva dal più ampio punto di vista dei numeri interi complessi.

Che i primi pitagorici siano in realtà «falsi primi» lo dimostra anche il fatto che è complicato dimostrare che ce ne sono infiniti: non si può adattare la famosa dimostrazione di Euclide dell'esistenza di infiniti numeri primi, che invece si adatta senza difficoltà ai primi non pitagorici. Supponiamo infatti che ci sia solo un numero finito di primi del tipo $4n + 3$, e consideriamo il numero N pari a 4 volte il loro prodotto, meno 1. Questo numero è del tipo $4n + 3$, ma ogni suo fattore primo è del tipo $4n + 1$: infatti, i primi del tipo $4n + 3$ dividono tutti $N + 1$, e dunque nessuno divide N.

La contraddizione si ottiene notando che il prodotto di numeri del tipo $4n + 1$ è ancora dello stesso tipo. Il che equivale, per il teorema di Natale, al fatto che il prodotto di somme di quadrati sia ancora una somma di quadrati: una proprietà scoperta da Diofanto, ma ovvia quando si ricordi il legame fra le somme di quadrati e le norme dei numeri complessi. Diversamente dai soliti regali di Natale, Fermat ce ne ha dunque fatto uno non solo bello, ma anche utile e duraturo.

Sheila Terry/SPL/Contrasto