di Piergiorgio Odifreddi

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

I numeri del frate

Nel XVII secolo Marin Mersenne identificò un insieme di numeri primi che erano quasi potenze di 2

Nel 1644, scorrendo la lista dei numeri primi noti fino ad allora, il frate Marin Mersenne si accorse che alcuni erano «quasi» potenze di 2. Si trattava dei cosiddetti «numeri primi di Mersenne», del tipo $2^m - 1$. Ai suoi tempi, non se ne conoscevano che sette: 3, 7, 31, 127, 8191, 131.071 e 524.287. I primi quattro erano noti fin dall'antichità. Il quinto era misteriosamente comparso verso la metà del Quattrocento, non si sa da dove. E il sesto e il settimo erano stati scoperti nel 1588 dal bolognese Pietro Cataldi, che nel 1603 li riportò nel *Trattato dei numeri perfetti*.

Questi numeri corrispondevano alle potenze di 2 di esponente 2, 3, 5, 7, 13, 17 e 19. Non a caso, tutti numeri primi anch'essi, visto che $2^{ab} - 1$ è divisibile sia per $2^a - 1$ che per $2^b - 1$, e non può essere primo. Per esempio, per $a = 2$ e $b = 3$ si ottiene 63, che è divisibile per 3 e per 7.

Detto altrimenti, un numero di Mersenne può essere primo solo se corrisponde a una potenza prima di 2. Ma, purtroppo, il contrario non è vero. Per esempio, già nel 1536 Ulrico Regio (Ulricus Regius) riportò nell'*Utriusque Arithmetices Epitome* che 11 è primo, ma 2047 è divisibile per 23 e 89.

Un filo logico

A questo punto, Mersenne si chiese per quali esponenti primi di 2 i suoi numeri risultassero primi. Non era facile trovare un filo logico in sette soli esempi, ma qualche regolarità c'era. A parte 2, che è pari, gli altri sei numeri si dividevano in due famiglie. Nella prima, i numeri 3, 5, 7 e 17 differivano di un'unità (in più o in meno) da una potenza di 2. Nella seconda, i numeri 13 e 19 differivano di tre unità (in più o in meno) da una potenza di 4. Mersenne generalizzò, e suppose che la lista dovesse continuare con 31, 67, 127 e 257. Nel 1772 Eulero annunciò in una lettera a Daniel Bernoulli che in parte Mersenne aveva ragione: il numero $2^{31} - 1 = 2.147.483.647$ era primo, e batteva il record mondiale di grandezza stabilito da Cataldi quasi due secoli prima. Per ottenere il suo primato, Eulero mostrò che i possibili divisori di quel numero potevano solo essere di due tipi molto particolari, e nessuno di essi funzionava.

Nel 1876 il francese Édouard Lucas trovò un semplice metodo per determinare se un numero di Mersenne è primo o no. Il responso fu che Mersenne aveva ragione anche su 127: questo stabiliva un nuovo record mondiale, che sarebbe durato altri 75 anni. Ma Mersenne aveva torto su 67, anche se il metodo di Lucas stabiliva solo indirettamente che $2^{67} - 1$ non è primo, senza mostrarne una fattorizzazione diretta. Questa dovette attendere il 31 ottobre 1903, quando lo statunitense Frank Cole fece un memorabile intervento a un convegno. Andò alla lavagna, e senza dire una parola calcolò in un'ora $2^{67} - 1$, da un lato, e il prodotto di 193.707.721 e 761.838.257.287, dall'altro. In entrambi i casi, il risultato fu 147.573.952.589.676.412.927. E Cole tornò al suo posto tra gli applausi.

Due problemi aperti

La lista di Mersenne era dunque sbagliata. Oggi sappiamo che i due numeri 67 e 257 erano da togliere. E che i tre primi 61, 89 e 107 andavano invece aggiunti. Per inciso, 61 è pari al cubo di 4, più 3: Mersenne avrebbe dovuto aggiungerlo fin dagli inizi, ma l'aveva dimenticato. In ogni caso, le sue condizioni non erano né necessarie, né sufficienti. In seguito si è cercato di precisarle in vari modi, con scarso successo. Usando raffinamenti del metodo di Lucas, finora si sono trovati una cinquantina di numeri primi di Mersenne, e ogni nuova scoperta costituisce un nuovo record.

Ma rimangono aperti due problemi. Il primo è se esistano infiniti numeri primi di Mersenne: cioè, infiniti primi p, con $2^p - 1$ primo. E il secondo, se esistano infiniti numeri pseudoprimi di Mersenne: cioè, infiniti primi p, con $2^p - 1$ non primo.