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

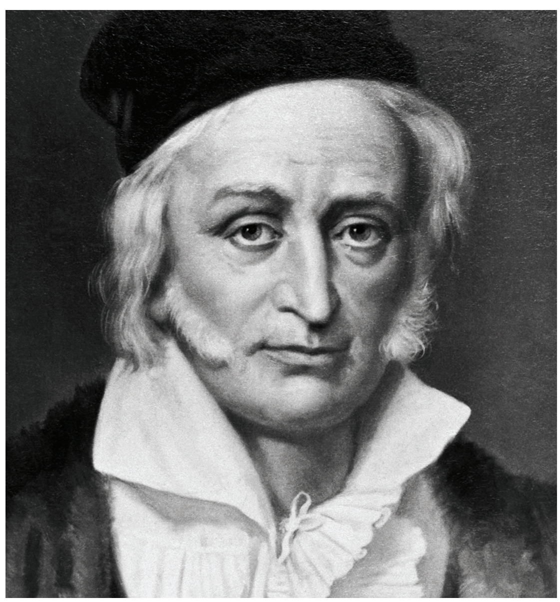
Un mondo in decomposizione

Per capire oggetti complicati basta ridurli a componenti canoniche più semplici

Uno dei teoremi più profondi e fecondi della matematica è la decomposizione unica (a parte l'ordine) dei numeri interi in fattori primi. L'esistenza della decomposizione è banale: basta continuare a dividere un numero in fattori sempre più piccoli, fino a quando non si arriva a fattori tutti primi. L'unicità invece è sorprendente, e riposa sulla Proposizione VII.30 degli *Elementi* di Euclide: se un numero primo divide un prodotto, divide anche uno dei fattori.

A causa della sua importanza la decomposizione unica in fattori primi è oggi chiamata teorema fondamentale dell'aritmetica, ma è stata enunciata esplicitamente soltanto un paio di secoli fa: precisamente, nell'articolo 16 delle *Disquisizioni aritmetiche* di Carl Gauss, scritte nel 1798 e pubblicate nel 1801. Ed è stato lo stesso Gauss a dimostrare, nel 1832, che una dimostrazione analoga prova anche la decomposizione unica per i cosiddetti interi complessi, corrispondenti ai punti di coordinate intere nel piano cartesiano.

Precisamente, gli interi complessi del tipo $m + in$ si possono decomporre in modo unico in interi complessi primi: cioè, non divisibili altro che per sé stessi e le quattro unità ± e $\pm i$, dove i indica la radice quadrata di meno 1. Con l'interessante conseguenza che alcuni numeri che sono primi come interi soliti, diventano composti come interi complessi: per esempio 2, che si può decomporre nel prodotto di $1 + i$ per $1 - i$.



Genio immortale. Il tedesco Carl Gauss è considerato come uno dei più grandi geni scientifici di sempre.

I tentativi di dimostrazione dell'ultimo teorema di Fermat portarono nell'Ottocento alla considerazione di numeri analoghi agli interi complessi, ma con sostituito dalla radice quadrata di un qualunque intero negativo fissato. Anche questi numeri si possono decomporre in fattori primi, ma non sempre in maniera univoca. Per esempio, 6 si può decomporre sia come 2 per 3, che come $1 + \sqrt{-5}$ per $1 - \sqrt{-5}$. E il motivo della doppia decomposizione è che il numero primo 2 divide il prodotto di $1 + \sqrt{-5}$ per $1 - \sqrt{-5}$, ma non divide nessuno dei due fattori.

Per ovviare al problema, nel 1843 Ernst Kummer introdusse i cosiddetti primi ideali, caratterizzati indirettamente attraverso la loro azione sui propri multipli, per il fatto che se dividono un prodotto allora dividono anche uno dei suoi fattori: allora la decomposizione, che non era unica rispetto ai fattori primi soliti, diventa unica rispetto ai fattori primi ideali. Nel linguaggio degli anelli commutativi introdotto nel 1876 da Richard Dedekind, l'idea di Kummer corrisponde a interpretare i vecchi numeri come ideali principali, estendere il discorso a tutti gli ideali, e provare che ogni ideale si può decomporre in maniera unica in ideali primi.

Arrivati a questo grado di astrazione, la decomposizione unica si può estendere anche ad ambiti ormai molto lontani dai numeri. Per esempio, ai polinomi in una variabile a coefficienti interi, che si possono decomporre in maniera unica in polinomi irriducibili: questi ultimi sono un analogo dei numeri primi, nel senso che non sono prodotti di polinomi non costanti. Oppure ai polinomi in una variabile a coefficienti complessi, nel qual caso il teorema fondamentale dell'algebra dimostrato da Gauss nel 1799 stabilisce che i polinomi irriducibili sono esattamente quelli di grado 1.

Salendo ancora di astrazione, anche i gruppi si possono decomporre in modo analogo al prodotto di due numeri, isolando al loro interno un sottogruppo normale N e identificando ciò che rimane con il gruppo quoziente G/N. I gruppi per cui una tale decomposizione non esiste si chiamano semplici, e costituiscono l'analogo dei numeri primi. Ogni gruppo finito ammette una decomposizione massimale in sottogruppi, ciascuno normale nel precedente, analoga alla decomposizione in fattori primi. E un teorema dimostrato da Camille Jordan nel 1869 e Otto Hölder nel 1889 dimostra che questa decomposizione è unica, come numero e struttura dei gruppi quoziente.

Ma una decomposizione unica in «fattori primi» esiste anche per oggetti matematici che, diversamente dai precedenti, non si possono facilmente assimilare a numeri. Per esempio, per i nodi da un lato, e per le superfici tridimensionali compatte e orientabili dall'altro, come dimostrato rispettivamente da Horst Schubert nel 1949 e John Milnor nel 1962. A testimonianza del fatto che la decomposizione è un approccio universale alla comprensione di oggetti complicati, mediante la loro sistematica riduzione a componenti canoniche più semplici.

Corbis