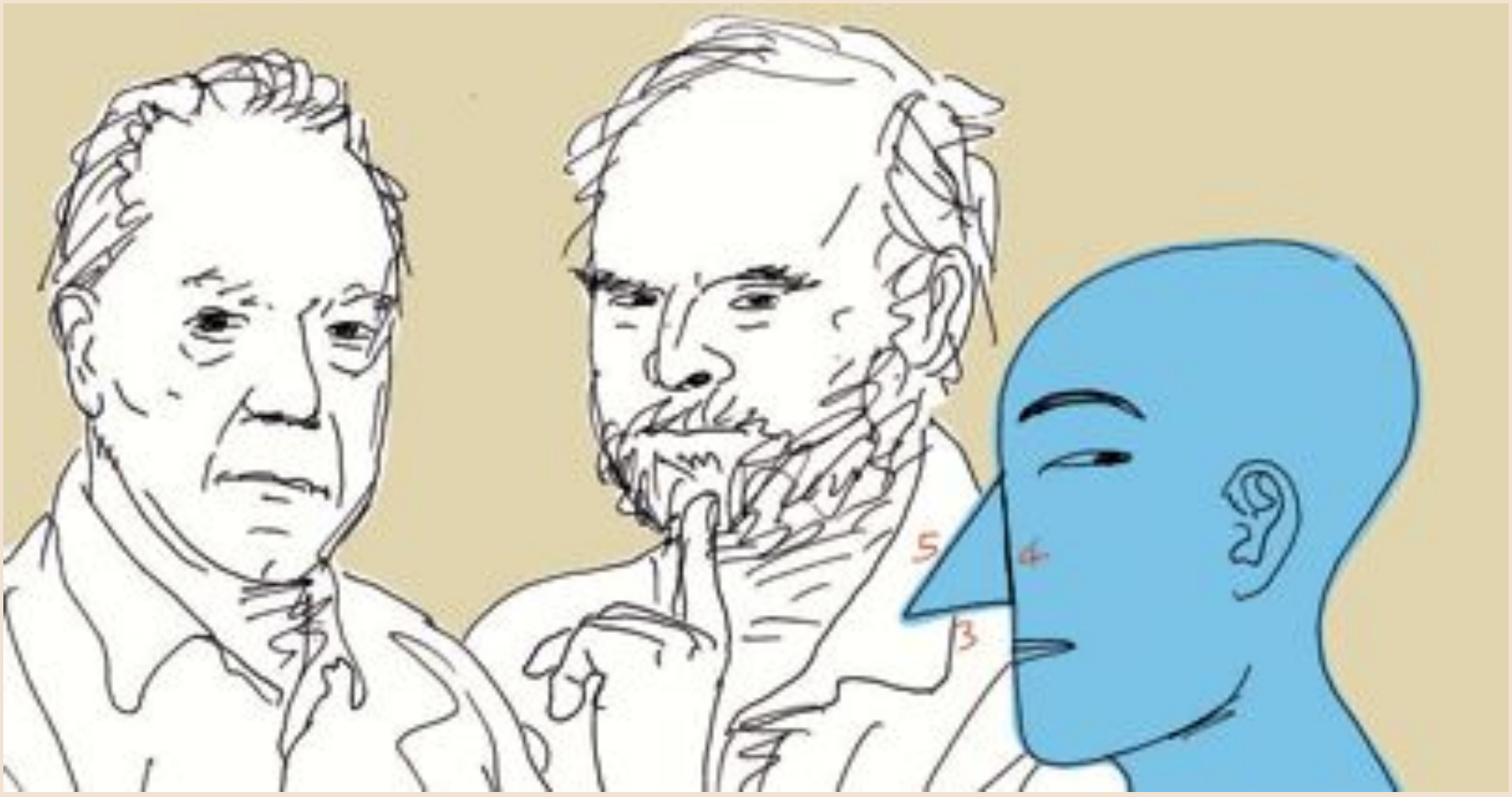
Il Sole 24 ORE

SCIENZA E FILOSOFIA

Matematica come serva e padrona

Vaughan F.R. Jones



Uno dei momenti di maggior perplessità per un matematico professionista è quando un profano innocentemente chiede: «Che cosa fate esattamente nel vostro lavoro?». Sarebbe davvero maleducato, e certamente controproducente per l'immagine della professione, rispondere: «Oh, non credo tu possa capire». Questa situazione è particolarmente imbarazzante su un aereo, dove si può avere questa persona accanto per diverse ore. Ho la fortuna – o sfortuna, non sono sicuro quale delle due – di avere la possibilità di replicare alla domanda con un po' d'idee di base sui nodi nello spazio tridimensionale e come il mio proprio lavoro abbia avuto un impatto sulla matematica. La questione fondamentale di «quando due nodi sono lo stesso» è abbastanza e intuitiva e non facile da comunicare con un po' di gestualità o anche con un pezzo di spago. Ma devo riconoscere che dopo una lunga spiegazione di questo tipo il mio interlocutore probabilmente penserà che io sia un po' pazzo, anche se veramente bravo ad allacciare le scarpe...

Ammettiamolo, quando si tratta di matematica, le persone di cultura media, e anche sopra la media, hanno imparato a scuola a risolvere l'equazione di secondo grado, forse anche a sommare una serie geometrica, ma nel giro di pochi anni dal termine dei loro studi hanno certamente dimenticato come fare tutte queste cose. I concetti necessari per spiegare la gran parte della ricerca matematica riguardante gli spazi di Hilbert, o le equazioni differenziali o le varietà compatte lisce, sono semplicemente impossibili da capire senza molte molte ore, e anche anni, di studio. Senza questa rigorosa preparazione, una persona, costretta a pensare in termini a lei comprensibili, sarà inevitabilmente portata a ritenere che i matematici fanno somme sempre più complicate aggiungendo e moltiplicando numeri sempre più grandi.

Non c'è molto che noi matematici possiamo fare al riguardo. In questo discorso cercherò di comunicare un po' del contagioso entusiasmo e dei modi di pensare ossessivi indotti dalla matematica, semplicemente parlando di somme sempre più complicate. Il titolo del discorso è *La matematica come schiava e come padrona* e vedremo due casi in cui essa viene usata in modo molto pratico e ripetitivo – matematica come schiava – e come allo stesso tempo una piccola curiosità possa condurre a una intensa riflessione indotta dal soggetto considerato. Così intensa che si viene coinvolti in una rete di pensieri ossessivi da cui non si esce fino a quando il problema è risolto – matematica come padrona.

Immaginate di essere un ingegnere nell'Egitto di circa 5.000 anni fa, con il compito di costruire una piramide a base quadrata. Gli angoli devono essere retti (cioè di novanta gradi) in modo estremamente accurato o l'intera costruzione non sarà stabile. Come si ottiene tale esattezza? I lati della vostra base quadrata potrebbero essere lunghi 200 metri, quindi un angolo retto formato a occhio ma su scala di circa un metro non sarebbe sufficientemente preciso. L'errore risulterebbe enorme. E, naturalmente, non disponiamo di alcun laser o teodolite visto che stiamo vivendo cinquemila anni fa. Ma un frammento di matematica astratta ci viene in soccorso, poiché è noto – il cielo sa come – che un triangolo i cui lati hanno lunghezze nel rapporto 3: 4: 5 ha un angolo retto. Non possiamo avere il laser, ma certamente abbiamo una corda e formare unità di misura che possono dunque essere facilmente misurate e possedere uguale lunghezza. Il sogno di un ingegnere. Perché l'errore nella determinazione dell'angolo retto sarà regolato da quello nell'uguaglianza delle unità di lunghezza della corda, che sarà a sua volta dovuto agli errori nel lavoro di taglio o piegatura della corda stessa. Così migliore sarà il lavoro, più piccolo sarà l'errore! Perfetto. Quindi andiamo avanti, costruiamo il nostro triangolo con corde con le proporzioni 3: 4: 5 e avremo un angolo retto perfetto come richiesto. Non resta che ripetere il processo per tutti gli angoli retti e per tutte le piramidi. La matematica è il migliore degli schiavi.

Ma i curiosi non possono fare a meno di pensare: «Ci sono altre combinazioni di numeri che funzionano come 3: 4: 5?». Sappiamo che la chiave è il teorema di Pitagora: in un triangolo rettangolo il quadrato costruito sull'ipotenusa è la somma dei quadrati costruiti sugli altri due lati. Così, se possiamo trovare altre terne di numeri interi tali che il quadrato del terzo sia la somma dei quadrati degli altri due abbiamo risolto il problema. Eventuali candidati? Consideriamo 5; 12 e $13.5^2 + 12^2 = 25 + 144 = 169 = 13^2$. Funziona, è affascinante. Ma è improbabile che possa essere di interesse per la costruzione di una piramide, la terna 3: 4: 5 è migliore sotto ogni aspetto. Meno unità corda, meno errori, meno tempo per costruire. Ma è intrigante, non è vero? Ci sono altre terne? Ne esiste una quantità infinita? C'è una formula che le fornisce tutte? Con il senno di poi, con cinquemila anni alle spalle, è facile considerare queste domande piuttosto facili. Ma a quei tempi la semplice manipolazione di numeri era più rudimentale, non esisteva l'algebra, il concetto di soluzione generale sarebbe probabilmente stato visto come una magia. Ognuna di queste terne pitagoriche sarebbe stata considerata mistica e, chissà, avrebbero potuto nascere sette religiose dedicate alla costruzione di nuove terne. Proviamo per esempio 8, 15 e 17. Funziona. Ma potrebbe non piacere l'idea che 15 e 17 dfferiscono di 2 e non di 1 come negli altri casi. Ci sono altri esempi senza questa proprietà? Le domande si accumulano una sull'altra e cercano una soluzione. Che può essere molto difficile. Non solo, tutto questo non ha alcuna applicazione pratica, visto che la nostra terna originale 3: 4: 5 rimane la migliore. Ma non possiamo fare a meno di porci queste domande, la matematica è diventata padrona. Così completamente che potremmo non essere in grado di sfuggire alla sua presa. Una soluzione a una domanda suggerisce solo un'altra domanda e così via, letteralmente all'infinito.

In effetti, la matematica è stata una schiavista formidabile in questo particolare problema. La nostra matematica moderna ha relegato la soluzione generale del problema delle terne pitagoriche a quello che noi chiamiamo in modo dispregiativo "banalità", ma questo non ci ha liberato dalla servitù. Infatti nel secolo XVII Fermat si è chiesto se esistono terne come 3, 4, 5

tali che la somma dei cubi dei primi due numeri sia pari al cubo del terzo: $a^3 + b^3 = c^3$. Egli ha rapidamente, anche se in modo estremamente intelligente, placato gli dei della matematica rispondendo al quesito e mostrando che tali terne non esistono. Ma allora come avrebbe potuto non chiedersi se le terne pitagoriche sono l'unica possibilità, ovvero se per nessun altro numero intero p esiste una terna con $a^p + b^p = c^p$? La matematica ha preso completamente il controllo, queste potenze superiori non sono né aree né volumi di qualche figura geometrica e quindi la domanda è del tutto slegata dalla costruzione di piramidi o dall'ingegneria. Ma è irresistibile per quelli di noi con una inclinazione alla matematica stessa. E così la padrona ha cominciato a spingere i suoi schiavi fino al limite. Ci vorranno più di tre secoli di profondo – davvero profondo – pensiero prima che gli dei della matematica siano nuovamente placati e Andrew Wiles dimostri "l'ultimo teorema di Fermat", utilizzando i più avanzati e astratti strumenti matematici disponibili.

La matematica può anche essere gentile con i suoi schiavi. Lo sviluppo di tutto ciò che è stato necessario nella teoria dei numeri per risolvere un problema del calibro dell'ultimo teorema di Fermat ci ha dato un notevole controllo di molte costruzioni dell'aritmetica. Questo controllo ha prodotto un importante strumento pratico nel campo delle comunicazioni e delle transazioni finanziarie: la crittografia a chiave pubblica. Questo è stato un concetto del tutto nuovo nell'eterno gioco di codifica e decodifica. Quando si invia un messaggio con chiave pubblica si trasmette a tutti la procedura esatta utilizzata per cifrare il messaggio (anche se non il messaggio stesso ovviamente). L'idea è che queste informazioni non sono di alcuna utilità per chiunque cerchi di decifrare il messaggio, a meno che abbia qualche informazione in più. Ci sono diversi metodi che possono essere utilizzati per ottenere questo risultato, ma il più noto è il metodo RSA. Esso fonda la sua sicurezza nella speranza che sia difficile fattorizzare un numero intero in prodotto di numeri primi. Ricordiamo che un numero primo è un numero intero che non ha fattori diversi da 1 e se stesso e che ogni intero può essere fattorizzato come un prodotto di primi in modo unico. Nel sistema RSA un numero viene reso pubblico e utilizzato per crittografare i messaggi. Questo numero è un prodotto di due primi piuttosto grandi, chiamiamoli p e q, ognuno dei quali è lungo diciamo 100 cifre. Il prodotto pq viene poi associato con la magia RSA al messaggio (anch'esso espresso da un numero) per la produzione di un altro numero che viene trasmesso al destinatario, e anche a chiunque altro che si dia la pena di ascoltare. Il trucco sta nel fatto che la decodifica del messaggio è facile (per un computer...) se si conoscono individualmente p e q e non solamente pq. L'unico modo per decodificarlo è decomporre pq nel prodotto dei due numeri primi, ma questo è un problema che richiede molto tempo, con i metodi conosciuti un tempo irragionevolmente lungo. Ma se il destinatario conosce p e q, il suo computer decodifica il messaggio velocemente.

Questa è nuovamente la matematica come schiava. Alcuni di questi metodi sono di ampio utilizzo nelle transazioni commerciali, per esempio con le carte di credito. Immaginate quanto spesso la schiava stia lavorando, giorno dopo giorno in tutto il mondo. Molto di più di quanto non fosse per il nostro ingegnere egiziano con il suo triangolo 3: 4: 5. Si può ben dire che vale quanto abbiamo speso. Ma, come nel caso delle terne di Pitagora, la matematica alla fine trionfa. Perché non si può fare a meno di chiedersi: «È proprio vero che la fattorizzazione di un numero è di per sé difficile?». La risposta è sì, questo problema è davvero complicato! A differenza delle terne pitagoriche e dell'ultimo teorema di Fermat rimane infatti irrisolto nonostante sforzi enormi e ossessivi. La matematica è nuovamente diventata padrona! E lo diventa ancora di più con il sogno del computer quantistico, un dispositivo che – ammesso che possa essere costruito – si avvarrebbe di qualche processo in parallelo inerente la meccanica quantistica per fare alcuni calcoli molto più velocemente di un computer convenzionale. Il computer quantistico richiede un nuovo tipo di matematica. Sorprendentemente, Peter Shor ha dimostrato che esso sarebbe in grado di fattorizzare un numero così rapidamente che il metodo RSA sarebbe inservibile! Il computer quantistico utilizzato in questo modo trasformerebbe la matematica di nuovo in schiava, ma la necessità pratica e la curiosità umana darebbero presto luogo a domande difficili le cui risposte richiederebbero ancora una volta la pedissequa e

maniacale devozione che sicuramente porterà a un altro uso della matematica come schiava. Il ciclo schiava- padrona continuerà fintanto che gli esseri umani esisteranno e continueranno a pensare, e anche per necessità.

Lectio Magistralis in occasione della Laurea Honoris Causa in Matematica conferita a Vaughan F.R. Jones, medaglia Fields nel 1990, (nel disegno, al centro), dall'Università di Roma Tor Vergata il 30 giugno 2016 su proposta di Roberto Longo. Jones ha definito l'ateneo romano «il centro mondiale della teoria algebrica dei campi quantistici» di cui Longo è il principale esponente.

24 LUGLIO 2016

TAG: Vaughan F.R. Jones, Roberto Longo, Andrew Wiles, Università Studi Roma "Tor Vergata", Peter Shor, Matematica, Cultura