LA MATEMATICA NELLA SOCIETÀ DI OGGI

di Enrico Bombieri *

Da sempre, scienza e società hanno lavorato insieme. In questo, la matematica certamente ha avuto un suo importante ruolo fin dal principio. La rappresentazione degli angoli in gradi sessagesimali, tuttora usata nella pratica, risale agli astronomi babilonesi. Le grandi piramidi dell'Egitto, con le loro proporzioni matematicamente esatte, hanno richiesto per la loro progettazione tecniche accurate di geometria e misurazione. Anche i primi matematici moderni hanno trovato motivazione nella pratica per i loro studi. Basta pensare all'introduzione del metodo della partita doppia in contabilità nel Quattrocento, e al ruolo dei matematici nel Cinquecento, al servizio dei principi per creare fortificazioni di città e tecniche di attacco e di difesa nella guerra. Col tempo, la scienza è cresciuta, il corpo di nozioni e di conoscenze raggiunte si è ingrandito al punto che la figura dello scienziato universale è scomparsa, e società e scienza hanno cominciato a separarsi. Diventa sempre più difficile spiegare al non esperto che cosa faccia la scienza odierna. Infatti, la scienza è diventata quantitativa, e descriverla in termini puramente qualitativi non basta per farsene un'idea realistica. Quindi, il parlare in termini vaghi di atomi, di elettroni, di protoni, di quarks, di quantum di energia non ci avvicina in modo particolare alla moderna fisica delle alte energie, così come il parlare genericamente di galassie e di quasars e di Big Bang non serve molto per comprendere realmente l'astrofisica di oggi. Né si può pensare che il parlare di doppia elica, di codice genetico, di genoma, di DNA basti per com-

* Institute for Advanced Study, Princeton.

prendere la biologia. Tuttavia il parlare, sia pure in termini generici, di queste cose ci fa vedere l'esistenza di un rassicurante collegamento diretto con la realtà, facendoci accettare più facilmente quelle parti che non comprendiamo. La situazione per la matematica è assai diversa, e il motivo è che l'oggetto di studio della matematica non è così tangibile e reale come per altre scienze. Per esempio, l'oggetto di studio della matematica non è il computer anche se spesso oggi si tende ad identificare le due cose. Quindi ci si domanda: che cos'è la matematica? A questa domanda, che mi sono posto molte volte, non è facile rispondere. La conclusione alla quale sono arrivato – certamente non definitiva e che probabilmente modificherò nel futuro – è che la matematica consiste nello studio delle relazioni tra oggetti diversi.

Ciò che importa è la relazione e la sua struttura interna; l'oggetto di per sé ha importanza solamente nella misura in cui si riflette nella relazione. Da ciò provengono l'enorme potere di astrazione della matematica e la sua straordinaria potenza di sintesi: oggetti molto diversi e in apparenza senza caratteristiche comuni possono diventare molto simili se esaminati dal punto di vista matematico. In altre parole, oggetti o gruppi di oggetti diventano matematicamente vicini se hanno relazioni simili. Per esempio, nella teoria dei controlli ciò che interessa è come agisce il controllo, e poco importa che cosa venga controllato.

La maniera più semplice di studiare in modo scientifico il mondo esterno consiste nell'osservazione: si accumulano dati mediante osservazioni, si scartano quelli che appaiono irrilevanti o di importanza secondaria, si conservano quelli significativi, e si ritorna alla lettura del materiale accumulato quando sia necessario. Questo modo di fare scienza si può paragonare allo scrivere una grande enciclopedia, aggiornando le nuove conoscenze acquisite e scartando le vecchie informazioni quando esse diventano superflue. Il suo scopo è utile, ma non sufficiente, poiché le informazioni raccolte in questo modo sono informazioni di riferimento, come in un dizionario, e non basta-

no di per sé per creare nuove idee, nuove direzioni, nuove intuizioni. Il punto debole di questo metodo è dovuto al fatto che non sappiamo a priori che cosa osservare, che cosa sia veramente interessante, che cosa vada conservato e che cosa vada scartato. A tutti noi è capitato, ricercando dati in un vecchio dossier, di notare che non c'è mai quello che cerchiamo, mentre ci sono molte informazioni ormai inutili; lo stesso avviene se esaminiamo vecchi libri di testo o vecchie enciclopedie. Quindi questo modo di fare la scienza non basta. Il seguente esempio è istruttivo. Quando il Pioneer Probe, una delle prime sonde spaziali, visitò il nostro sistema solare, si ritenne opportuno mandare indietro dalla sonda alla Terra una grandissima quantità di dati, che furono registrati su migliaia di nastri magnetici. L'idea era che dall'esame di questi dati sarebbe stato possibile ottenere nuove informazioni sul nostro sistema solare. In realtà la maggior parte dei dati raccolti non fu mai esaminata, perché non si sapeva cosa farsene. Oggi la tecnologia di raccolta dei dati è cambiata al punto tale che non vi è più un computer (tranne forse qualche macchina nello Smithsonian Museum) in grado di leggere i nastri del Pioneer Probe.

L'altro modo di fare scienza è per procedimento induttivo. Di nuovo i dati vengono raccolti e analizzati. Questa è una fase essenziale del procedimento scientifico: la scienza, e anche la matematica, deve avere collegamento con la realtà, con il mondo in cui viviamo. Adesso però questi dati vengono esaminati con uno scopo preciso: scoprire caratteristiche comuni di aspetto e di comportamento, cercando leggi generali che governano l'evoluzione di complicati sistemi. Piuttosto che formare teorie distinte, una per ogni sistema preso in esame, si formano principi unificanti e generali. In un certo senso, la formulazione di leggi generali è come il buon senso, basato più sull'esame in grande delle strutture di base che attraverso l'esclusivo esame del particolare e del contingente. La scienza di base e con essa la matematica – che definitivamente è una scienza di base – utilizzano in modo essenziale questo metodo induttivo.

Vi è un altro aspetto della matematica astratta, oltre a quel-

lo di fornire uno strumento eccezionalmente duttile per trasformare concetti in quantità misurabili della precisione voluta, e cioè la matematica in quanto scienza che può studiare se stessa. La matematica, diversamente dalle altre scienze, può trovare in se stessa la motivazione per porre nuovi problemi, creando nuovi rami con lo scopo di unificare concetti distanti e scoprendo nuovi e impensati collegamenti tra oggetti matematici in apparenza diversi. Come in un racconto di Borges, la matematica, studio delle relazioni tra oggetti, trasforma le relazioni stesse in oggetti matematici, che sono pertanto messi in relazione tra loro, creando relazioni tra relazioni, quindi nuovi oggetti, e così via all'infinito. Non è qui la sede per approfondire questo argomento con le sue implicazioni logiche e filosofiche, ma basterà accennare solamente che un ramo della matematica, la teoria delle categorie, si occupa anche di questi problemi.

In questo panorama matematico emergono problemi e congetture, quasi come distanti catene montuose che ci chiamano alla scalata delle loro vette. Le teorie matematiche, risultato di costruzioni, si possono paragonare a opere architettoniche – palazzi, torri, strade, ponti – con una loro interna bellezza, simile a quella della musica e delle arti figurative, una volta che diventi comprensibile il linguaggio nel quale la matematica si esprime. Molti matematici pensano alla matematica come un mondo con una sua realtà, dove il matematico ha il ruolo di esploratore di terre lontane e sconosciute. In parte, questa visione è corroborata dal fatto che le nuove conoscenze matematiche si aggiungono continuamente al cumulo delle conoscenze passate: il passato viene raramente messo da parte, anche se a volte una nuova teoria rimpiazza procedimenti più tortuosi, così come il tunnel del Monte Bianco ha rimpiazzato difficili valichi alpini. Possiamo affermare con sicurezza che la matematica è una scienza conservatrice, senza grandi rivoluzioni nel corso della sua storia.

La matematica astratta segue, nel suo sviluppo, un criterio di linearità, che il matematico motiva spesso con ragioni di

tipo estetico. André Weil, uno dei più grandi matematici viventi, vede la matematica come Michelangelo vedeva la scultura, fatta di un materiale duro e difficile dal quale occorre rimuovere il superfluo. Così come la scultura è già contenuta nel blocco di marmo grezzo, la matematica è anch'essa contenuta nella totalità delle relazioni logiche; l'opera del matematico consiste nell'eliminare le relazioni inutili. Questo ci serve a capire il ruolo dell'intuizione e della motivazione estetica nella matematica. A ogni passo, occorre scegliere tra un numero enorme di possibilità. Dovendo scegliere tra il semplice e il complicato, tra la via diretta e la via indiretta, il teorico procede sempre con il rasoio di Occam, tagliando il difficile. Ma allora la matematica resta sempre pura astrazione, arte e intuizione? Sicuramente no. Anche la matematica più astratta, motivata da considerazioni intuitive ed estetiche, ha profondi collegamenti con il mondo reale e spesso trova origine e ispirazione in altre scienze e nella tecnologia.

Matematici come Von Neumann, Gödel, Einstein, per menzionare quelli più noti, ma anche Riemann, Hilbert, Poincaré e molti altri, hanno così cambiato il nostro modo di pensare in aree quali la fisica, la logica, la filosofia. Il loro influsso nella scienza in generale è stato enorme.

Ci si può domandare: ha importanza tutto questo? È assai probabile che se Einstein non avesse scoperto la relatività, questa sarebbe stata ugualmente scoperta, magari attraverso tanti piccoli contributi di svariati scienziati, messi finalmente insieme in un tutto coerente. Oppure si potrebbe argomentare che se Turing non avesse avuto l'idea di una macchina calcolatrice universale, e se Von Neumann non avesse creato il primo grande computer a tubi elettronici in grado di eseguire programmi, certamente il computer sarebbe stato messo insieme da qualche parte, sia pure un poco dopo. Ma questo punto di vista è irrilevante. Il fatto è che dove e quando avvengono scoperte fondamentali ha grandissima importanza nello sviluppo di una nazione. La scienza è fatta dall'uomo e non procede da sola in maniera automatica.

Vi sono molti istruttivi esempi di parti astratte della matematica che hanno trovato e continuano a trovare applicazioni nel mondo reale. Il primo importante esempio è quello dei gruppi di Lie e della topologia. I gruppi di Lie – non occorre qui definirli in termini precisi – si possono pensare come fatti di simmetrie, considerando come simmetrie non solo la tipica riflessione in uno specchio, ma anche simmetrie più generali, quali le rotazioni, dilatazioni e altre ancora più complesse. I gruppi di Lie appaiono dappertutto in matematica e fisica e hanno un ruolo fondamentale nella fisica atomica. I matematici hanno scoperto che, sorprendentemente, ci sono relativamente pochi gruppi di Lie e sono riusciti a descriverli e studiarli esplicitamente in grande dettaglio. La loro importanza proviene dal fatto che in un gruppo di Lie si può fare l'analisi matematica, compreso il calcolo differenziale e integrale di Newton e Leibnitz, con la differenza che adesso lo spazio ambiente non è lo spazio piatto euclideo ma è un gruppo di Lie con curvatura, che può essere molto più vicino alla realtà di quanto lo sia la geometria euclidea. L'analisi armonica in questi spazi corrisponde a quello che negli spazi euclidei ci dà la scomposizione di fenomeni periodici in una sovrapposizione di frequenze elementari di diverse fasi e ampiezze.

Un'applicazione pratica dell'analisi armonica su un gruppo di Lie è la TAC, la tomografia assiale computerizzata. Nella TAC si fanno molte radiografie di un oggetto da tutte le direzioni, ottenendo dati che sono l'immagine bidimensionale radiografata sulla lastra sensibile. Non occorre in realtà che l'immagine sia fisicamente su una lastra di vetro o una pellicola di gelatina, infatti nella pratica questi dati sono raccolti in forma digitale in un computer. Il problema è quello di ricostruire l'oggetto a tre dimensioni a partire dalla conoscenza delle varie immagini a due dimensioni. Possiamo pensare alla lastra fotografica, orientata nella direzione voluta, come a un piano nello spazio. Ora i piani nello spazio a tre dimensioni formano quello che i matematici chiamano uno spazio omogeneo per un gruppo di Lie, nel nostro caso la varietà Grassmanniana dei

piani dello spazio; il problema di ricostruzione dell'immagine è un problema di analisi armonica, il problema di Radon, dal matematico che lo ha considerato per primo oltre settant'anni fa. La risoluzione teorica del problema consiste in una generalizzazione della trasformata di Fourier, già nota da tempo. La risoluzione pratica del problema di Radon è stata resa possibile dal computer, con un programma di software, la FFT, cioè la Fast Fourier Transform, introdotta negli anni '60 da Winograd con l'IBM. La FFT ha permesso di effettuare in tempo reale i complessi calcoli che compaiono nel problema di Radon. Solamente allora la ricerca teorica è pronta per l'uso in campo tecnologico, con le molteplici applicazioni in campo medico note a tutti. Il procedimento simile di Risonanza Nucleare Magnetica dipende da tecniche matematiche vicine, anche se la fisica sottostante dipende da principi completamente diversi; con la TAC, forma un buon esempio di oggetti differenti con relazioni matematiche simili. In questo caso, l'applicazione della matematica è resa possibile solamente dall'uso simultaneo di teorie diverse, quali l'analisi armonica in un gruppo di Lie e la trasformata di Fourier unita a raffinate tecniche di scienza del computer e tecnologia.

Un altro esempio, non importante ma che bene illustra l'ubiquità dei gruppi di Lie nella matematica, è quello del movimento di tre segmenti rigidi articolati tra loro, quale potrebbe essere un autotreno con rimorchio. Questo movimento è descritto per mezzo di un'equazione differenziale il cui gruppo di simmetrie è il gruppo eccezionale di Lie chiamato G_2.

Un esempio importante del procedimento inverso, cioè come la matematica venga motivata dall'esterno, è la matematica discreta, cioè quella in cui l'oggetto fondamentale di studio è il discontinuo piuttosto che il continuo. Fanno parte della matematica discreta l'analisi combinatoria e la teoria dei grafi (cioè dei vari modi di collegare punti fra loro), rami che hanno avuto un enorme sviluppo nell'ultimo ventennio, dovuto in larga parte al loro potenziale per applicazioni pratiche e immediate nei settori del computer e delle comunicazioni.

I corpi finiti hanno un'importanza speciale nella matematica discreta. L'esempio più semplice consiste delle due classi pari-dispari, un corpo finito con due elementi: si pensi ai bit 0-1 del computer. Più in generale, le classi di resti per la divisione per un numero primo formano un corpo finito. Negli anni tra il 1940 e il '50 i matematici si sono accorti che si poteva fare la geometria su un corpo finito in maniera molto simile alla geometria classica. Per molto tempo questi studi sono stati considerati tra gli aspetti più esoterici della matematica astratta, comprensibili solo dagli addetti ai lavori e privi di applicazioni pratiche. Oggi la situazione è cambiata. All'inizio degli anni '80 il matematico russo Goppa è riuscito a costruire un nuovo tipo di codici, utili per la trasmissione efficiente di dati, a partire da curve modulari su corpi finiti. Più recentemente sono stati ottenuti grafi, i cosiddetti magnifiers e expanders, con caratteristiche di efficienza vicinissima alla massima efficienza teorica. La storia di questi grafi è particolarmente interessante e merita una breve digressione.

Supponiamo di voler costruire una rete telefonica efficiente, un problema di alto interesse pratico. Possiamo visualizzare questa rete come un grafo, i cui vertici sono i centralini di smistamento, connessi con lati, che sono le linee telefoniche che collegano i centralini. Si vuole che la rete sia robusta, cioè anche se un centralino si guasta o ha troppo lavoro c'è un modo facile per far passare ugualmente le telefonate attraverso altri centralini, e si vuole anche che la rete telefonica sia economica, cioè che possa portare molte telefonate usando relativamente poche linee. Una rete è efficiente se è robusta ed economica nello stesso tempo.

Il grado di un grafo è il massimo numero di lati uscenti da un vertice: grado basso vuol dire meno linee e quindi economia. D'altra parte, la robustezza si ottiene facendo sì che un gruppo di vertici si colleghi con molti nuovi vertici vicini. Più grande il rapporto di queste due quantità, più efficiente è la rete; le reti in cui il rapporto è grande sono i magnifiers. In un magnifier l'informazione può essere trasmessa in tutta la rete con grande rapidità.

Fortunatamente, una rete telefonica fatta a caso risulta spesso ragionevolmente efficiente. Ma, in un mondo competitivo quale l'industria odierna, non basta. Occorre essere più efficiente degli altri, guadagnando margini di sicurezza e aumentando la propria competitività. Anche un guadagno del 5% in efficienza sulla concorrenza può significare la dominanza di un mercato. I primi tentativi di costruire i magnifiers mediante regole precise furono una delusione: tutti i grafi ottenuti erano inefficienti. Paradossalmente, era come se fosse meglio costruire un supercomputer con circuiti a caso piuttosto che con una architettura precisa. Finalmente, lavori recenti di Margulis, Alon, Milman, Lubotzky, Phillips e Sarnak hanno cambiato le cose e adesso abbiamo a disposizione regole precise per costruire i magnifiers. Basta menzionare la matematica coinvolta in queste ricerche: per primo, un analogo discreto della equazione di Laplace, un'equazione introdotta alla fine del Settecento da Laplace in una memoria sugli anelli di Saturno, e che si incontra ovunque nello studio dell'elettricità, magnetismo, gravità, elasticità, astrofisica, ma che uno non si sarebbe mai immaginato in questo contesto; poi, la costruzione del grafo stesso, partendo da uno spazio omogeneo per un gruppo di Lie, e dividendo per un sottogruppo discreto; infine, risolvere l'equazione discreta di Laplace sul grafo concludendo, attraverso l'ipotesi di Riemann nei corpi finiti (uno dei risultati più profondi di tutta la matematica), che il grafo in questione è essenzialmente ottimale.

Queste ricerche, rese possibili solo attraverso l'uso della matematica astratta, hanno il potenziale di passare utilmente nella pratica. Ma la loro vera importanza consiste nell'averci dato un nuovo modo di studiare i grafi. Le vere applicazioni pratiche sono nel futuro, nei supercomputer con centinaia di migliaia, se non addirittura milioni, di processori, e nell'intelligenza artificiale, dove le linee corrispondono ai neuroni che collegano i gangli nervosi, o addirittura ai pensieri che collegano le diverse caratteristiche di un oggetto o di classi di oggetti. Si può pensare a un computer costruito con un superproces-

sore non fatto con milioni di transistor collegati tra loro in modo preciso e determinato a priori, bensì con miliardi di transistor in cui i collegamenti vengono ottenuti non copiando disegni predeterminati ma procedendo invece in maniera diversa per ogni processore, attraverso un procedimento di software che scarta automaticamente gli inevitabili transistor difettosi, escludendoli dai collegamenti. In questo modo, diventa possibile superare il problema di controllo della qualità di un insieme così grande di transistor. Il computer così ottenuto può addirittura avere circuiti ridondanti. Pur non sapendo come sia fatto esattamente il processore, tuttavia esso funzionerà ugualmente con perfetta efficienza, come la famosa "scatola nera" della scienza del computer, un oggetto teorico che garantisce un certo funzionamento e del quale non sappiamo nulla della sua struttura interna e di come lavora.

Un aspetto di queste ricerche è stato quello di avere stimolato studi assai profondi sul comportamento di grafi formati a caso, che hanno chiare applicazioni nello studio di grandi modelli più aderenti alla realtà di quanto lo siano modelli deterministici.

La matematica astratta ricava molte delle sue idee dall'esterno. Un esempio importante è come il computer abbia dato origine a una nuova branca della matematica, la teoria della complessità.

Fino a poco tempo fa, i matematici teorici consideravano un problema risolto se esisteva un metodo conosciuto, o algoritmo, per risolverlo; il procedimento di esecuzione dell'algoritmo era di importanza secondaria. Probabilmente il motivo di questo atteggiamento di indifferenza era dovuto al fatto che dovendo fare i calcoli a mano o questi erano assai facili da fare oppure erano totalmente impraticabili. Il computer ha cambiato completamente questo quadro. Adesso, è importantissimo trovare metodi di soluzione che siano pratici per il calcolo. La teoria della complessità studia i vari algoritmi e la loro relativa efficienza computazionale.

Molti problemi hanno una complessità catastrofica (espo-

nenziale): si pensi al gioco degli scacchi. Un'analisi completa di due mosse è in media di almeno 100 casi, tre mosse 1000, 6 mosse un milione di casi. Con 13-14 mosse, cioè 6-7 mosse di un giocatore, si raggiungono i limiti dei supercomputer odierni e di quelli futuri, se ci vogliamo limitare a un programma che analizza tutte le possibilità. Il grande maestro di scacchi procede in modo diverso, più scientifico, analizzando i motivi fondamentali presenti nel gioco, riconoscendo in base a questi le strategie possibili, scegliendo infine una linea di gioco che sembra promettente. Al momento, i migliori programmi di computer per gli scacchi procedono per forza bruta: i programmi si distinguono tra loro per la velocità di esecuzione e per il modo di valutare la bontà di una posizione. Il giorno in cui il computer arriverà a includere nel suo programma il riconoscere le numerose strutture fondamentali del gioco, non attraverso regole fissate in precedenza, bensì attraverso l'uso di pochi principi generali, allora avremo la macchina veramente imbattibile, che avrà superato la barriera della complessità esponenziale.

L'importanza della teoria della complessità non deriva certo dal suo uso nell'analisi di giochi come la dama o gli scacchi; essa ha una motivazione eminentemente pratica, in quanto per il computer la complessità misura il tempo necessario per eseguire un programma, e quindi bassa complessità è sinonimo di brevità di esecuzione e, pertanto, di efficienza e di basso costo. Ma le applicazioni di questa teoria vanno oltre: un esempio è in un problema pratico di grande importanza, quello della sicurezza dei dati.

Viviamo un periodo della storia dell'umanità paragonabile a quello della rivoluzione industriale, e precisamente la rivoluzione delle comunicazioni. Attraverso la radio, la televisione, il telefono possiamo metterci in contatto istantaneo con tutto il mondo. Si può immaginare una rete telefonica così avanzata che ogni persona abbia un telefono portatile, che permetta chiamate ovunque e da qualunque posto. I dati di transazioni commerciali si riversano istantaneamente nei banchi di memo-

ria dei computer; i traffici e gli spostamenti di aerei, treni, navi sono noti e seguiti in tempo reale; attraverso il computer, possiamo consultare istantaneamente i dati anagrafici e le caratteristiche personali degli impiegati, e così via.

Se non vogliamo trasformare questo mondo e questa società in un mondo orwelliano è fondamentale che l'accesso alla banca dei dati sia strettamente limitato alle persone autorizzate, relativamente ed esclusivamente alla parte che si deve accedere, garantendo la confidenzialità dei dati. Inoltre, cosa fondamentale, i dati non devono essere modificabili o cancellabili tranne che con procedure garantite e precise.

Al giorno d'oggi, l'unico computer sicuro da influenza esterna è il computer isolato che lavora con un singolo utente. Tuttavia l'utilità vera del computer non consiste soltanto nell'elaborazione dei dati, ma anche nel far parte di una rete di comunicazione, quale quella che si trova all'interno dell'impresa o addirittura, come nel mondo scientifico, a livello mondiale. Lo sviluppo dei metodi di informazione rende possibile svolgere attività quali la spesa al supermarket, operazioni di banca, transazioni commerciali, attraverso il telefono. Ma come si può garantire l'identità di una persona attraverso il telefono? Qual è il documento di identità che è sicuro? Come garantire che il messaggio che mandiamo è ricevuto dalla persona giusta? In altre parole, come garantire la sicurezza? I casi riportati dai giornali mostrano che siamo ben lontani dall'averla ottenuta.

La sicurezza viene garantita a vari livelli: limitazioni nell'accesso, parole d'ordine, dati registrati in crittografia. Tuttavia non è pratico avere un sistema in cui occorre un sistema speciale per ogni coppia di utenti. Quello che si vuole è un sistema per spedire un messaggio sicuro, in cui ogni utente ha per codificare una sua chiave, che è pubblica, come i numeri sull'elenco del telefono.

Vi è pertanto molto interesse nella crittografia con chiave pubblica. L'idea è di avere un sistema per codificare-decodificare nel quale la conoscenza della chiave per codificare

non aiuta per nulla nel decodificare, e viceversa. Possiamo paragonare un tale sistema a un labirinto accessibile soltanto attraverso una botola di pubblico accesso: si entra facilmente attraverso la botola, ma una volta entrati non si può più uscire per la stessa via, e uscire dal labirinto è impossibile senza la mappa. Per essere un sistema pratico, questo sistema deve essere capace di grandi variazioni, in modo che ogni utente abbia un procedimento personalizzato per codificare-decodificare: ricevere il corretto messaggio cifrato equivale a una firma di autenticità, che corrisponde in modo unico all'utente.

Supponiamo ora che un'impresa produca un software per effettuare tutto ciò. Questo software viene venduto in tutto il mondo ed è adottato dalle grandi imprese e dai governi. Tutto funziona alla perfezione per qualche anno fino a che succede il disastro: un gruppo di matematici trova un modo originalissimo per scoprire la chiave del sistema, col risultato di creare scompiglio ovunque. Esiste un modo per vedere in anticipo se un tale programma di software sia sicuro?

Recentemente sono stati proposti alcuni programmi in questo senso, basati sulla teoria dei numeri. Uno dei più popolari è basato sul fatto che mentre è facilissimo moltiplicare due numeri, è difficilissimo scomporre un numero in un prodotto di fattori. Dieci anni fa, scomporre un numero di 30 cifre in fattori era considerato impensabile. Oggi esistono metodi assai complicati (alcuni coinvolgono la geometria sui corpi finiti) con i quali si fattorizzano numeri fino a 45 cifre in un personal computer. Un supercomputer fattorizza agevolmente numeri di 70 cifre, e una rete di workstation (forse i futuri supercomputer) fattorizza numeri di 100 cifre. Di recente, una rete di 1500 computer ha fattorizzato un numero di circa 150 cifre, che rappresenta un po' il record fino a oggi. Quanto deve essere grande una chiave per essere sicura? La risposta dipende dalla complessità teorica del problema della fattorizzazione, la cui determinazione è un problema tuttora aperto.

Il problema della sicurezza dell'informazione è duplice. Infatti, la disponibilità di metodi crittografici semplici e pratica-

mente impossibili da decifrare senza conoscerne la chiave solleva preoccupazioni di vario genere. Cosa succederebbe se le imprese tenessero due libri contabili, un libro ufficiale e un libro nero segreto, nascosto nei banchi di memoria di un grande computer, e irriconoscibile come tale tranne a chi ne possiede la chiave? Oppure metodi per convertire la voce in segnali digitali, crittografarli e spedirli su una comune linea telefonica, per essere decifrati all'arrivo per mezzo della chiave segreta? Questo permetterebbe l'organizzazione del crimine in modo informatico, con risultati disastrosi per la società in cui viviamo. Una proposta, che ritengo di valore assai dubbio, approvata di recente e quasi in segreto dal governo degli Stati Uniti, è quella di standardizzare il metodo di crittografia in un procedimento noto solo al governo e non all'utente. Il governo, dopo l'approvazione di un magistrato, ha così la possibilità di decifrare qualunque dato crittografato da chiunque. Ogni altro sistema di crittografia è dichiarato illegale, con severe pene per chi ne fa uso. Finché il sistema sociale si mantiene democratico e le garanzie costituzionali dell'individuo sono presenti, le conseguenze di un tale sistema possono essere quasi invisibili. Tuttavia nessuno può garantire che una democrazia rimanga sempre tale e che il potere, già assai grande, dello Stato non si trasformi in abuso. La possibilità che lo Stato si trasformi in Big Brother diventa realtà. Sta ai legislatori e ai sociologi risolvere questo conflitto, di sempre maggiore attualità, tra libertà dell'individuo e sicurezza dello Stato.

In un mondo reale non occorre sempre riuscire nel 100 per 100 dei casi, e talvolta avere successo nella maggioranza dei casi ci può bastare. Nel caso del problema della sicurezza del computer, riuscire in un caso su 10.000 a scoprire la chiave basterebbe a rendere inutile un sistema di protezione usato su larga scala. Questo conduce a problemi di tipo probabilistico sulla complessità, con un comportamento spesso assai diverso da quello di tipo deterministico: un esempio classico è l'algoritmo del simplesso in programmazione lineare, che ha complessità deterministica esponenziale, ma che ha complessità probabili-

stica polinomiale. Si tratta cioè di un algoritmo che funziona benissimo nella pratica, con rarissime eccezioni. Tutti questi problemi rappresentano parti importanti della matematica la cui origine risale all'esterno della matematica stessa.

Negli ultimi anni sono stati fatti grandi progressi nello studio dell'evoluzione di fenomeni e di sistemi complessi che hanno caratteristiche di quasi periodicità. Ogni cosa che è controllata dall'esterno, ma che ha in sé la capacità di influenzare l'esterno, è un sistema dinamico che può presentare caratteristiche imprevedibili nella sua evoluzione. Gli esempi sono ovunque: l'alternarsi delle stagioni, in prima approssimazione periodico ma in realtà sempre diverso, l'ecosfera con la sua popolazione predatore-preda-cibo, il sistema immune dell'uomo, tutti i sistemi economici di una certa scala.

La prima impressione è di caos: si forma un comportamento in apparenza ordinato che però si distrugge rapidamente, seguito da un nuovo comportamento simile ma diverso, con analogo comportamento fugace, un po' come le nubi nel cielo in una giornata di vento o come le oscillazioni del listino di borsa. Quando ci sembra di aver osservato qualche periodicità, e ci azzardiamo a far previsioni, il nostro sistema dinamico cambia di nuovo comportamento in modo inaspettato. I matematici hanno scoperto che sistemi dinamici di natura dissipativa possono essere descritti per mezzo di pochi casi tipici, e hanno fatto notevoli progressi nello studio di questi ultimi. Il problema principale al momento è quello di predire il comportamento di un sistema dinamico su una grande scala di tempo, descrivendo i modi tipici di comportamento. Per esempio, il moto di un punto in un sistema dinamico può essere: periodico o quasi-periodico (tornando allo stesso punto a intervalli regolari, o tornando nelle vicinanze a intervalli più o meno regolari), ergodico (muovendosi quasi a caso, ma visitando nel tempo ogni posto), o ancora più complicato.

Molto interessante è anche l'evoluzione di sistemi dinamici con variabili stocastiche, in cui l'evoluzione avviene non in modo rigorosamente deterministico, ma solamente con una

certa probabilità; questi sistemi dinamici sono certamente più idonei a descrivere situazioni reali. Il risultato di questi studi, appoggiati da un nuovo tipo di matematica che si potrebbe definire matematica sperimentale, mostra che l'evoluzione dei sistemi dinamici è ancora più complessa di quanto possa apparire da simulazioni sul computer. Un altro aspetto metodologico importante è l'abbandono dell'approccio col binomio *teorema-dimostrazione*, con una catena logica mai interrotta di ragionamenti ferrei, includendo ogni tanto, o anche molto spesso, il binomio *simulazione sul computer-plausibile comportamento*. Si giunge addirittura a considerare algoritmi che hanno solamente una certa probabilità di funzionare, con risultati che hanno solamente una certa probabilità di essere esatti.

Alcuni problemi fondamentali di ingegneria e matematica applicata sono ancora troppo grandi per un attacco diretto con metodi teorici, e troppo grandi per un attacco con l'esperimento o anche con la simulazione con il computer. La dinamica dei fluidi viscosi ne è l'esempio tipico.

Ancora non sappiamo se le equazioni di Navier-Stokes, che risalgono a oltre un secolo fa, diano o no un modello adeguato del movimento dei fluidi viscosi, come aria, acqua o petrolio. Capire la turbolenza è un problema di grande importanza pratica, data la grande energia che viene dispersa nel moto turbolento; le cause della turbolenza sono ancora incognite. Risolvere il problema della turbolenza significa poter costruire automobili, aerei, navi più efficienti. Significa anche migliori motori a combustione, controllando la miscelazione aria-benzina; vi sono collegamenti con la diffusione dei fluidi in setti porosi, quali per esempio depositi di petrolio in terreni sabbiosi, o infiltrazioni di scarichi industriali in una falda acquifera. E significa anche predizione del tempo più accurata su scala più grande. Infatti, la matematica della dinamica dei fluidi è rilevante in altre questioni, quali il moto e la struttura delle galassie, la formazione e la stabilità del plasma nelle macchine a fusione nucleare, la formazione di interfacce nella crescita di cri-

stalli, che chiaramente è fondamentale nella tecnologia dei semiconduttori.

Il progresso in quest'area proviene da una fusione di tecniche teoriche, sperimentali e di simulazione. Il computer di per sé non basta: occorre un buon modello su cui lavorare. Ma un modello adatto per bassa velocità, bassa viscosità e bassa compressibilità potrebbe non essere più realistico a velocità supersonica. A questo livello, la teoria aiuta a scegliere un modello migliore, che però, di per sé, non basta a risolvere il problema. A questo punto entra in gioco la simulazione con il computer, che studiando sperimentalmente il nuovo modello ci fa comprendere meglio la teoria attraverso l'analisi dei risultati, e se i risultati confermano le prove sperimentali, abbiamo fatto un passo avanti. La teoria può e deve a questo punto fare predizioni, da confermarsi con la simulazione e la sperimentazione. Questo delicato gioco sta portando i suoi frutti, ed è piuttosto recente la conferma sperimentale che il moto laminare dei fluidi, il più efficiente, può essere mantenuto a velocità anche alte se le superfici dei materiali sono perfettamente lisce e della forma giusta; le previsioni sono di una riduzione del 30% nei consumi di carburante nei futuri aerei.

Altri metodi matematici nuovi sono per esempio la teoria delle ondelette, che è molto più adatta, per calcoli numerici con il computer, della vecchia analisi di Fourier. La teoria delle ondelette è adesso usata con successo dalla ricerca petrolifera nell'analisi dello scattering di onde di shock per individuare i giacimenti.

Osservando storicamente lo sviluppo della matematica e le sue applicazioni si vede che le prime applicazioni importanti sono arrivate quando lo sviluppo industriale ha portato una nuova tecnologia di maggior precisione. Le applicazioni alle altre scienze sono arrivate tipicamente con una distanza di trenta-cinquant'anni. Tale è la distanza di tempo fra la teoria delle forme differenziali e le equazioni di Maxwell dell'elettromagnetismo, e tale è la distanza di tempo tra l'invenzione delle geometrie di Riemann e la loro applicazione data da Einstein

alla relatività generale. I codici di Goppa sono però a vent'anni di distanza dallo studio delle curve modulari sui corpi finiti, e il lavoro di Phillips-Sarnak-Lubotzky sui grafi segue di soli dieci anni i lavori di Deligne sull'ipotesi di Riemann sui corpi finiti. L'impressione è ben chiara: il divario di tempo tra teoria e applicazione si sta riducendo sempre più.

In un mondo estremamente competitivo come quello dell'industria di oggi, in una società che deve integrarsi in una comunità sempre più ampia, un mondo in cui è necessario ottenere le risposte ai quesiti sempre più rapidamente, la matematica ha una duplice funzione: la ricerca di modelli di studio su cui elaborare i dati in maniera consistente, e la verifica che il risultato dell'elaborazione corrisponda allo scopo che si era prefisso. Per esempio, possiamo studiare con i metodi più rigorosi e avanzati un modello econometrico, ma è altresì necessario vedere in modo quantitativo, e non solo qualitativo, che i risultati corrispondano alla realtà. Questa seconda parte è a mio parere essenziale se si vuole dare validità alla ricerca. Per esempio, lo studio di logiche a più valori, di logiche anomale, – oggi di moda nel campo dell'informatica – è utile solo se corrisponde a una realtà, magari distante nel futuro, di applicazione all'informatica.

Non è necessario per tutti avere a disposizione un ufficio studi di matematici pronti ad analizzare qualunque cosa. Le grandi industrie del computer, le grandi compagnie telefoniche, le grandi banche e compagnie di assicurazione ne hanno bisogno, così come la grande industria che utilizza la simulazione computerizzata in grande scala per la progettazione. La piccola impresa deve tuttavia trovare, attraverso consulenze opportune, il modo di restare aggiornata e di tener continuamente presente che l'ottimizzazione della produzione e del lavoro si fa ormai su base scientifica.

Vi sono due difficoltà. La prima è quella della preparazione di matematici che non siano solamente dei teorici, ma che al contrario non rifuggano dai contatti con l'industria per l'ispirazione di temi di ricerca. Se non vogliamo separare la scienza

dalla società, occorre la formazione di scienziati che siano in grado di lavorare a metà strada tra teoria e industria. Le nostre strutture universitarie sono inadeguate e i programmi di insegnamento vanno riveduti. La maggior parte dei matematici riceve nell'università una preparazione di tipo accademico, spesso non bene motivata e che ha fine in se stessa. È necessario creare un nuovo ruolo per il matematico, che lo renda in grado di lavorare direttamente nel quadro dell'industria. Questo matematico farà necessariamente parte di un gruppo di ricerca, e la ricerca matematica per l'industria sarà necessariamente ricerca di gruppo.

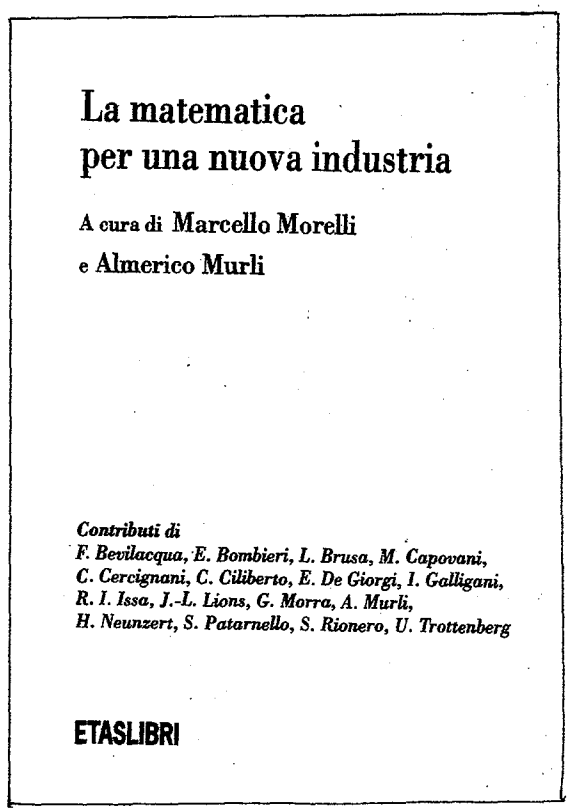
L'altro problema che secondo me sta diventando molto serio, è quello di evitare di produrre un esercito di superspecialisti. Occorrono anche i generalisti. La specializzazione a un livello prematuro produce effetti positivi immediati, quali la possibilità di rapido impiego con buon rendimento iniziale, ma a lungo termine crea persone prive di quella elasticità mentale che è necessaria se un'industria vuole evolversi al passo richiesto dalla società moderna. La tecnologia avanzata di oggi è la tecnologia superata di domani, e solamente persone con ampia preparazione di base potranno effettuare i cambiamenti necessari con facilità, meglio ancora anticiparli. Al momento, le grandi aree dove la matematica si applica all'industria sono la modellistica e la simulazione, l'ottimizzazione, il calcolo scientifico e tecnico, la gestione e l'elaborazione dei dati, la gestione dei servizi. Nessun campo è escluso, dall'aeronautica alla zootecnia.

Ma allora dobbiamo concludere che la matematica può essere applicata ovunque? La risposta è chiara. Se la matematica è, come credo, lo studio delle relazioni tra oggetti occorre, prima di applicarla, capire le relazioni stesse. In sostanza, occorre avere tutti i termini dell'equazione prima di pensare di risolverla. Una matematica applicata alla sociologia, alla politica, alla finanza internazionale richiede anzitutto di capire il tessuto interno di queste materie. La storia dimostra che siamo ben lontani dal poterlo fare e dal comprendere il ruolo dell'elemento

umano in esse, e i tentativi di dare un contenuto matematico a queste materie non sono finora, a mio parere, molto incoraggianti.

Nel futuro, si può prevedere che lo strumento matematico, attraverso l'informatica e il computer, entrerà sempre di più a far parte della nostra società. Ma non credo che la matematica si spezzerà in due, matematica astratta e matematica applicata: parafrasando il motto di Pasteur sulla scienza, non esiste la matematica applicata, ma piuttosto l'applicazione della matematica.

Questo articolo del 1994 è tratto dal seguente libro


La matematica
per una nuova industria

A cura di Marcello Morelli
e Almerico Murli

Contributi di
F. Bevilacqua, E. Bombieri, L. Brusa, M. Capovani, C. Cercignani, C. Ciliberto, E. De Giorgi, I. Galligani, R. I. Issa, J.-L. Lions, G. Morra, A. Murli, H. Neunzert, S. Patarnello, S. Rionero, U. Trottenberg

ETASLIBRI