ACCADEMIA NAZIONALE DEI LINCEI

ADUNANZA GENERALE SOLENNE

10 giugno 2016

Enrico Bombieri

La matematica: indispensabile strumento per lo sviluppo della società

Da sempre, scienza e società hanno lavorato insieme. La mente umana, con la sua capacità di astrazione e con la sua capacità di memoria sia singola che collettiva, è in grado di semplificare l'esperienza fino al punto di formulare le leggi della natura e della logica, in una continua ricerca della conoscenza e della verità.

Possiamo immaginare la nascita della geometria come conseguenza della necessità, in una società tribale e non nomade, di misurare e dividere equamente la terra e di costruire abitazioni, strade, e luoghi adeguati per le cerimonie pubbliche e religiose. Mi piace pensare che il primo teorema formulato dall'uomo è il fatto che un triangolo con lati 3, 4, e 5, è un triangolo rettangolo, precisamente l'angolo più semplice che appare in una costruzione. Personalmente, ho visto un giardiniere usare questo metodo per delimitare una aiola rettangolare di media grandezza. A questo aggiungiamo il cerchio, la riga e il compasso ed otteniamo l'inizio della geometria euclidea.

La geometria piana non è unico appannaggio della cultura della Grecia antica e la troviamo nelle culture indiane e cinesi. È importante osservare che, indipendentemente, problemi astratti ma fondamentali sollevati dallo studio della geometria piana, quali la natura del numero Pi Greco (area del cerchio di raggio 1), sono stati risolti soltanto con metodi elevati della matematica moderna. A questo proposito, mi piace ricordare Dante nei versi dell'ultimo canto del Paradiso nella sua Commedia:

“Qual è ’l geometra che tutto s’affige
per misurar lo cerchio e non ritrova,
pensando, quel principio ond’elli indige,”

paragonando i vani tentativi dei matematici per comprendere la natura di Pi Greco alla sua incapacità di comprendere il mistero teologico della Trinità. Vani tentativi infatti, dato che nel 1882 il matematico Lindemann dimostrò che Pi Greco non si può ottenere con una costruzione finita nel quadro della geometria euclidea.

Un altro esempio di impossibilità, questa volta noto alla scuola pitagorica, è il fatto che la diagonale di un quadrato non è commensurabile con il lato del quadrato. Questa scoperta diede origine ad innumerevoli controversie filosofiche sulla natura dei numeri.

Nell’antichità, l’interazione della matematica con il mondo esterno trova la sua migliore espressione con Archimede. Come matematico fu il precursore del calcolo infinitesimale, con la quadratura della parabola e il calcolo dell’area della sfera che risulta uguale a quella del cilindro circoscritto alla sfera, un teorema che Archimede stesso considerava come il suo più grande risultato. Racconta Cicerone che, quando era questore a Siracusa, scoprì in mezzo ai rovi la perduta tomba di Archimede per via di una pietra posta su un pilastro, nella quale era stata scolpita l’immagine di una sfera racchiusa da un cilindro. Allo stesso tempo, l’ingegnere e fisico Archimede formulò la teoria delle leve (datemi un punto di appoggio e vi solleverò il mondo), inventò gli specchi ustori per difendere Siracusa dall’attacco della flotta romana, e formulò le prime leggi dell’idraulica.

Il retaggio della matematica greca fu largamente conservato ed esteso dalla cultura araba nel periodo aureo del califfato musulmano e riportato in Europa da Leonardo Pisano, detto il Fibonacci, con il suo *Liber Abaci* e il *Liber Quadratorum*. In questo periodo, l’introduzione dei numeri negativi e dello zero come numero (lo zero non è il nulla!) fu una pietra miliare per lo sviluppo dell’aritmetica. Il metodo della partita doppia di Luca Paciolo diventò un essenziale strumento per il commercio. La geometria, attraverso il trattato nel Quattrocento di Leon Battista Alberti sulla pittura, nel quale sviluppa la geometria prospettiva con un punto all’infinito, ebbe una enorme influenza nella pittura ed architettura in Europa.

La fine del Quattrocento e il Cinquecento videro la matematica andare ben oltre l'aritmetica e la geometria e la nascita dell'algebra, un altro contributo importato dal mondo arabo. La soluzione in formule algebriche dell'equazione cubica da parte di Tartaglia, dell'equazione del quarto grado fatta da Scipione dal Ferro sono un'altra pietra miliare nella storia della matematica. In alcuni casi, le formule risolutive richiedevano la radice quadrata di numeri negativi, anche se le soluzioni erano espresse con numeri reali. Il passo fondamentale e rivoluzionario, fatto dal Bombelli poco dopo, fu di legittimare la radice quadrata di un numero negativo come "numero immaginario", tuttavia trattabile algebricamente come veniva fatto con i numeri reali. Questo passo che ha ampliato la nozione di numero è oggi alla base della matematica moderna.

Il Seicento vede la nascita del calcolo differenziale e integrale con Cavalieri, Leibniz, Newton, e la loro applicazione alla nuova fisica iniziata da Galileo e dalla rivoluzione copernicana, e con Napier vede l'introduzione del logaritmo naturale e della sua base, il nuovo numero e = 2.71828…, considerato da Napier il moltiplicatore di un capitale investito al 100%, ma ad un interesse composto calcolato in maniera continua.

Il numero e diventa il quarto numero fondamentale della matematica, dopo il numero 1, Pi Greco, e l'immaginario $i = \sqrt{-1}$, legati tra loro da quello che considero la più straordinaria equazione della matematica, cioè la relazione di Eulero $e^{2\pi i} = 1$ che lega tra loro l'aritmetica (il numero 1), la geometria (Pi Greco), l'algebra (la radice quadrata di –1), e l'analisi (il numero e, ottenuto con un limite).

Il Settecento è dominato dalla figura di Eulero, vero matematico universale e fondatore di interi settori della matematica, sia astratta sia applicata allo studio delle leggi fondamentali della natura.

Inizia così una fruttuosa interazione tra la matematica, scienza essenzialmente astratta, e la fisica, la scienza che descrive il mondo in cui viviamo. Eulero, che ritengo essere il più grande matematico di tutti i tempi e il vero fondatore della matematica moderna, trova le equazioni che descrivono la meccanica dei fluidi, pone le basi della moderna teoria dei numeri, dell'analisi combinatoria, della teoria delle equazioni differenziali e della geometria differenziale, pone i fondamenti dell'analisi numerica, e compie i primi passi della topologia. Laplace formula la fondamentale equazione che descrive l'equilibrio di un sistema dinamico. Ugualmente importante e innovativa è la pubblicazione del volume *Ars Conjectandi* di Bernoulli, che contiene la prima base del calcolo delle probabilità.

In un'altra direzione, d'Alembert, interpretando un'onda come sovrapposizione di onde elementari di flusso e riflusso ottiene l'equazione differenziale a derivate parziali che descrive un'onda. Poco dopo, Fourier scopre che qualunque fenomeno periodico si può descrivere come sovrapposizione di onde elementari semplicissime. Il riconciliare le due descrizioni, matematicamente assai diverse, ha portato a risultati profondi in analisi che ultimamente sono culminati in applicazioni pratiche, ad esempio nella medicina.

Queste ricerche nel campo dell'analisi al giorno d'oggi formano i grandi settori delle equazioni differenziali a derivate parziali, della analisi armonica, e del calcolo delle probabilità.

Questi risultati non solo furono ampliati, ma infatti seguiti da una vera esplosione della ricerca matematica in nuove direzioni. Algebra, geometria, logica matematica, analisi combinatoria, teoria dei numeri, topologia, probabilità e l'analisi stocastica, sono adesso ad un livello così avanzato che diventa difficile per un matematico lavorare in più di un settore. Uno si domanda: Cosa è in realtà la matematica? Questa è una domanda che mi sono posto più volte, giungendo alla fine alla conclusione che la matematica è la scienza delle relazioni tra oggetti astratti. Lo strumento essenziale è la verità logica e gli oggetti stessi sono frammenti di verità logica. Così come un quadro non è soltanto un aggregato di particelle colorate, ma infatti acquista un suo significato intrinseco (siamo vicini al concetto di aspetto di Wittgenstein), così l'oggetto matematico diventa una entità con una identità propria.

La scienza moderna col tempo è cresciuta enormemente, al punto che la figura dello scienziato universale, come Aristotele, Leonardo, o Newton, è scomparsa e società e scienza hanno cominciato a separarsi. Diventa sempre più difficile spiegare al non esperto di cosa si occupa la scienza moderna. La scienza è diventata quantitativa e descriverla in termini puramente qualitativi non basta per farsene un'idea realistica. Parlare in termini vaghi di elettroni, protoni, quarks, quantum di energia non ci avvicina alla comprensione della fisica delle alte energie, così come le parole galassia e quasar non bastano per comprendere l'astrofisica. Lo stesso avviene per la biologia: le parole doppia elica, codice genetico, genoma, DNA, non bastano per farci una idea di cosa sia in realtà la biologia moderna.

Nella matematica, ciò che importa è la relazione e la sua struttura interna: l'oggetto, o gli oggetti messi in relazione, ha importanza solo nella misura in cui si riflette nella relazione. Da qui provengono l'enorme potere di astrazione della matematica e la sua straordinaria capacità di sintesi: oggetti molto diversi ed in apparenza senza caratteristiche in comune possono diventare molto simili se esaminati dal punto di vista matematico. Un esempio di natura pratica si trova nella teoria dei controlli: quello che interessa è il modo di agire del controllo, ed è di minore importanza ciò che viene controllato.

Esiste un altro aspetto della matematica che la distingue dalle altre scienze: la matematica è una scienza che può studiare se stessa. Come nella *Biblioteca di Babele* di Borges, la matematica, studio delle relazioni tra oggetti, trasforma le relazioni stesse in nuovi oggetti che sono messi in relazioni tra loro, creando così nuovi oggetti, e così all'infinito. La teoria delle categorie si occupa di questo e, ben lungi dall'essere un gioco astratto, ha trovato applicazione in algebra e geometria.

In questo panorama matematico emergono problemi e congetture, come distanti catene montuose che ci chiamano alla scalata delle loro vette per scoprire cosa c'è oltre. Le teorie matematiche, che sono il risultato delle costruzioni del matematico, si possono paragonare ad opere architettoniche, palazzi, torri, strade, ponti, con una interna bellezza paragonabile a quella della musica o delle arti figurative una volta che sia acquisito il linguaggio esoterico della matematica. Nello sviluppo della matematica astratta troviamo un criterio di linearità che spesso ha un fondamento estetico. André Weil, uno dei più grandi matematici del ventesimo secolo, vedeva la matematica come Michelangelo vedeva la scultura, nascosta dentro un materiale duro e difficile dal quale occorre eliminare il superfluo. Così come la scultura è contenuta nel blocco di marmo grezzo, così la matematica è contenuta nell'enorme blocco delle relazioni logiche; l'opera del matematico consiste nell'eliminare le relazioni inutili. Dovendo scegliere tra la via diretta e quella indiretta, il teorico procede con il rasoio di Occam, tagliando il difficile.

Ma allora, la matematica è solo pura astrazione, arte e intuizione? Sicuramente la risposta è un sonoro no. Anche la matematica più astratta, motivata da considerazioni intuitive ed estetiche, ha profondi collegamenti con il mondo reale e spesso ha origine 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 cambiato il nostro modo di pensare in aree quali la fisica, la logica, e la filosofia. Ci si può domandare: ha importanza tutto questo? È probabile che se Einstein non avesse scoperto la relatività, essa sarebbe stata scoperta magari attraverso osservazioni e piccoli contributi da parte di molti scienziati, e 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 computer a tubi elettronici in grado di eseguire programmi, certamente il computer sarebbe stato messo insieme da qualche parte, sia pure un poco dopo. A mio parere, osservazioni di questo tipo sono irrilevanti. Il fatto è che dove e quando avvengono scoperte fondamentali ha grandissima importanza nello sviluppo di una nazione, ed è altresì importante notare che le grandi scoperte della scienza sono sempre precedute da molte piccole scoperte che formano il terreno fertile dal quale nascono le grandi idee. Questo terreno fertile si forma nelle scuole per i giovanissimi ed è necessario individuare gli studenti estremamente dotati e guidarli adeguatamente. Abbassare il livello di insegnamento al fine di raggiungere livelli prestabiliti di successo non è il modo migliore di guidare le eccezioni. La scienza è fatta dall'uomo e non procede da sola in maniera automatica.

Vi sono molti esempi di parti astratte della matematica che hanno trovato, e continuano a trovare, importanti applicazioni nel mondo reale. Un esempio importante è la teoria dei gruppi di Lie, dal matematico norvegese Sophus Lie che li introdusse e studiò sistematicamente alla fine dell'Ottocento. i gruppi di Lie – non occorre qui di definirli in modo preciso – si possono pensare come un insieme di trasformazioni effettuate in modo continuo. Ad esempio, la totalità delle rotazioni di un cerchio o di una sfera formano gruppi di Lie. Questi gruppi appaiono dappertutto in matematica e fisica, ad esempio sono essenziali nella fisica dell'atomo. Il fatto sorprendente è che ci sono relativamente pochi gruppi Lie ed i matematici sono riusciti a descriverli con grande dettaglio. In un gruppo di Lie si può fare l'analisi matematica, compreso il calcolo differenziale e integrale di Leibniz e Newton, con la fondamentale differenza che lo spazio ambiente non è più lo spazio piatto euclideo ma uno spazio curvo, assai più adatto a descrivere la realtà fisica.

Un successo della matematica moderna è la generalizzazione dell'analisi armonica cominciata da Fourier, questa volta fatta in un gruppo di Lie. Un esempio famoso di applicazione di questa matematica alla medicina è la TAC, cioè la tomografia assiale computerizzata.

La TAC ci permette di ottenere una immagine tridimensionale precisa avendo a disposizione un numero sufficiente di radiografie prese da direzioni diverse. Il problema matematico che corrisponde a questo è il problema di Radon, il matematico ungherese che lo considerò quasi cento anni fa. Data una funzione in tre variabili, è possibile ricostruirla conoscendo il valore dell'integrale della funzione lungo una retta arbitraria, per tutte le rette?

La totalità delle rette nello spazio è quello che i matematici chiamano una varietà grassmanniana, dal matematico Grassman che studiò la geometria di oggetti di questo tipo già nell'Ottocento. Le varietà grassmanniane si descrivono per mezzo dei gruppi di Lie. Radon ottenne la risoluzione del problema utilizzando l'analisi armonica su i gruppi di Lie, per mezzo di una formula chiamata in suo onore la trasformata di Radon.

Il passaggio dalla teoria alla pratica spesso è difficile. Occorrevano due cose: la prima, approssimare il problema, conoscendo l'integrale della funzione lungo le rette ma solo per le rette avente origine in un numero finito di punti (l'origine dei raggi X), e la seconda era il calcolo veloce della trasformata di Radon, il che era un problema di ben altra natura. Solamente con l'avvento del computer e un nuovo metodo rivoluzionario per il calcolo numerico, la FFT (Fast Fourier Transform, introdotta da Winograd all'IBM negli anni 60), la TAC divenne realtà e strumento essenziale della medicina moderna.

Questo è un buon esempio di come parti apparentemente disgiunte della matematica (geometria, analisi, algebra e teoria dei numeri per la FFT) si fondono insieme per ottenere grandi risultati. Altri metodi quali la RNM e il PetScan sono basati su una fisica assai diversa da quella dei raggi X, ma la matematica necessaria per l'analisi dei dati osservati è essenzialmente la stessa.

La teoria della relatività generale di Einstein è fondata sulla geometria differenziale di Riemann e sul calcolo differenziale assoluto di Ricci Curbastro, che la precedono di molti decenni. Nel senso opposto, la fisica quantistica ha indicato ai matematici, con l'equazione di Schrödinger e l'equazione di Dirac, due nuove equazioni differenziali fondamentali quanto l'equazione di Laplace o l'equazione delle onde. Più di recente, l'interazione tra matematica e fisica è diventata sempre più stretta. La nuova teoria della fisica detta la teoria delle stringhe cerca di fondere insieme la fisica dell'atomo e la fisica dell'universo e ha proposto nuovi metodi di studio. Le nuove idee introdotte dai fisici hanno portato alla soluzioni di molte questioni aperte nella matematica e sono tuttora all'avanguardia della ricerca.

Infatti, la matematica non è una collezione di teoremi disgiunti l'uno dall'altro, e non è nemmeno una collezione di problemi risolti o da risolvere. La matematica descrive il tessuto complesso ma coerente della verità logica e da qui proviene la sua flessibilità per la sua applicazione allo studio del mondo in cui viviamo.

Il calcolo combinatorio, iniziato nel Settecento per contare il numero di disposizioni di un insieme di oggetti ma soggette ad opportune condizioni, è oggi cresciuto al livello di una nuova ampia branca della matematica con importanti applicazioni pratiche, dal fare programmi efficienti per il computer allo studio di circuiti quali una rete stradale o la struttura dell'Internet. Parte essenziale del calcolo combinatorio è la teoria dei grafi. Un grafo è semplicemente un insieme di punti (i nodi), alcuni dei quali sono connessi da segmenti (i lati), che possono anche essere percorsi in una sola direzione. Ad esempio, la rete stradale dell'Italia è rappresenta da un grafo, con nodi gli incroci stradali e lati le strade tra nodi. Un grafo è connesso se non si può scomporre in due pezzi separati tagliando una connessione, ed è robusto se occorrono molti tagli per sconnetterlo. Una rete stradale è robusta se nel caso delle chiusura di una o più strade si può ovviare all'inconveniente dirottando il traffico su altre strade.

Da qui la domanda: è possibile costruire un grafo robusto con molti nodi e pochi lati? La risposta a questa domanda è interessante. Infatti, un grafo con lati scelti a caso, diventa robusto a partire da una certa soglia minima per il numero di lati, ma solo di recente usando profondi metodi della matematica moderna è stato possibile costruire esplicitamente grafi robusti con pochi lati.

Allora, sarà possibile snellire il traffico di Roma usando la teoria dei grafi? La difficoltà consiste nel fatto che il traffico non è uniforme, le strade hanno ampiezza varia, il traffico consiste non solo di veicoli, ma anche di pedoni e i veicoli hanno conducenti che decidono di testa sua quando cambiare direzione, accelerare o fermarsi. Al momento, la matematica non è (a mio parere, fortunatamente) in grado di trovare una soluzione teorica ottimale per tutto questo, ma già ci sono simulazioni di circolazione automatica di veicoli stradali senza conducente e senza semafori, applicando anche tecniche matematiche che hanno origine dallo studio del movimento dei fluidi iniziato da Eulero. Ma tutto questo appartiene al futuro.

La teoria della probabilità al giorno d'oggi pervade le scienze sociali e la sua applicazione alla statistica è fondamentale. La legge di Gauss, che misura la probabilità di deviazione dalla media, si applica dovunque. Ma la legge di Gauss si applica sempre? La risposta è no. Come osservato dalle grandi compagnie assicurative, le grandi deviazioni dalla media sono più frequenti di quanto predetto dalla legge di Gauss. La simulazione sul computer era troppo lenta per trovare le leggi esatte per la probabilità di eventi straordinari. Solamente di recente i matematici hanno scoperto che cambiando la scala del fenomeno in maniera adatta la legge di Gauss continuava a valere. Il cambiamento di scala in questione è assai complicato e lontano dall'essere evidente e questo spiega come mai questo non sia stato scoperto prima. Oggi, questa scoperta ha permesso di analizzare e simulare sul computer eventi straordinari che non potevano essere analizzati con i metodi usuali, che richiedevano un tempo eccessivo per l'apparizione di questi eventi.

Anche nella matematica astratta la teoria della probabilità è diventata fondamentale, poiché è in grado di garantire l'esistenza di un oggetto matematico con determinate proprietà senza il bisogno di darne una costruzione esplicita, funzionando come quello che in gergo comune è chiamato "una scatola nera", un oggetto che ha determinate proprietà ma non sappiamo come è fatto dentro e come funziona. Questo ha portato alla soluzione di difficili problemi, di natura non solo teorica. In alcuni casi, la soluzione probabilistica resta la sola soluzione nota: si sa che esiste una soluzione con tutte le proprietà richieste, ma non siamo in grado di descrivere esattamente come è fatta. Questo può apparire sorprendente, ma dal punto di vista logico la difficoltà si può descrivere con il principio dei cassetti: se sappiamo che abbiamo messo tre oggetti in due cassetti, possiamo dedurre che un cassetto deve contenere almeno due oggetti, ma non siamo in grado di dire quale cassetto li contiene.

Il computer di oggi, con la sua potenza e rapidità di analizzare ed elaborare dati, insieme alla sua abilità di eseguire programmi assai complessi, ha realizzato la macchina universale di Turing e sta trasformando rapidamente la struttura sociale mondiale. Combinato con la rivoluzione delle comunicazioni e dei trasporti, e con la nuova straordinaria abilità di accumulare ed esaminare dati, ha cambiato l'abilita dell'uomo di accumulare l'informazione, sia buona che cattiva, e di farne uso. A questo punto si pongono importanti domande.

Nel campo della finanza mondiale, la matematica sta svolgendo un ruolo nuovo in particolare nell'automazione del mercato delle transazioni di borsa, nel quale si arriva al punto di migliaia di transazioni in una frazione di un secondo. Qui il rischio è ben descritto dalla legge di Bombieri sulla finanza (Bombieri il banchiere, mio padre): "I profitti sono numeri su un pezzo di carta, le perdite sono in contanti". Il computer, per conto suo, non è in grado di distinguere tra le due cose e il misurare il vero rischio non è ancora una scienza.

Consideriamo l'Internet, oggi diventato il tessuto che unisce l'informazione. Dal punto di vista matematico, l'Internet è un grafo i cui nodi sono i punti dove l'informazione viene ricevuta e smistata. È l'Internet un grafo robusto? La risposta è ambigua. Da un certo punto di vista, lo è. Localmente, l'informazione può essere trasmessa in più modi. Se uno dei tanti computer di una linea aerea non funziona, di solito è possibile in un tempo non eccessivo dirottare l'informazione su un altro computer. Tuttavia, l'informazione passa anche attraverso centri specializzati (ad esempio, satelliti di comunicazione) che sono vitali per tutto il sistema. Questo rende l'Internet vulnerabile su grande scala.

La notizia che una grande potenza sta facendo oggi esperimenti per distruggere satelliti artificiali (ormai inutili e non funzionanti) per mezzo di un suo satellite armato di potenti raggi laser, è venduta al pubblico come una cosa utile ma in realtà ci presenta la possibilità di una nuova arma militare per interrompere le comunicazioni, cosa essenziale in guerra, come è noto a chiunque abbia fatto il servizio militare.

Su scala minore ma con effetto diretto per tutti, si sono già verificate altre situazioni: attacchi attraverso un numero eccessivo di richieste di continuo accesso creando così seri problemi di funzionamento, ed anche attacchi fatti da altre nazioni usando gruppi militari di esperti per passare oltre la barriera di sicurezza dei computers di grandi aziende, ottenendo dati segreti sulla produzione, e addirittura infiltrandosi nei computers di agenzie governative. Vediamo qui la matematica, o l'applicazione della matematica, al servizio dello spionaggio internazionale.

Un'altra area dove la matematica moderna ha portato grandi risultati è l'analisi dei dati. I dati vengono classificati in base a certe caratteristiche, in generale più di una e quindi appartenenti a quello che un matematico considera come uno spazio a più dimensioni. La difficoltà è che l'esplorazione di questo spazio si fa per esempio un dato alla volta, vale dire con una curva nello spazio. Nel 1890, il matematico Peano fece una scoperta che va contro l'intuizione: una curva continua che riempie tutto il piano. Considerata una volta come una stranezza, una curiosità matematica, la curva di Peano e le sue varianti sono alla base di metodi per costruire una curva, nel senso ordinario, che passa vicino a ogni punto dello spazio. Assegnando ai dati varie proprietà selezionate in ordine di importanza si ottiene una nozione di distanza nello spazio dei dati e la curva esplora rapidamente, nell'ordine di importanza dovuto, un enorme database. Sistemi di ricerca sull'Internet come Google usano idee di questo tipo, così come è per il marketing e anche per l'antiterrorismo.

A questo punto vi sono due problemi. Il primo è la sicurezza dei dati: limitazione all'accesso e limitazione alla lettura. Il secondo, l'abuso dell'informazione.

Nel primo problema si usano parole d'ordine e registrazione crittografata dei dati, facili per chiunque da crittografare ma difficilissimi da leggere in chiaro. Per la seconda parte, un sistema in uso comune si basa sui numeri primi: è facilissimo moltiplicare due numeri molto grandi (diciamo cento cifre) ma difficilissimo scomporre il prodotto in fattori che sono numeri primi. Si può paragonare un sistema di questo tipo ad un labirinto da cui si entra facilmente attraverso una botola che viene poi chiusa ermeticamente, ma da cui è difficilissimo uscire. In questo campo, i matematici sono avanti ai fisici, avendo dimostrato che un computer (teorico) che segue le leggi della meccanica quantistica renderebbe inefficace un sistema di comunicazione basato sulla fattorizzazione. Al momento, i fisici non sono in grado di costruire un computer quantistico, ma l’ultima parola in proposito non è stata ancora detta.

Il matematico inglese Hardy, grande specialista della teoria dei numeri, scrisse che lui amava la teoria dei numeri perché non poteva avere applicazioni militari. Oggi le cose sono cambiate, non solo per quanto riguarda le applicazioni militari ma anche per il fatto che diventa sempre più vicino il momento in cui la profezia Orwelliana del Grande Fratello può diventare realtà. Sta alla società moderna porre i giusti limiti all’uso di questi metodi in modo che siano di utilità comune e non vengano abusati a scapito della libertà individuale.

Le accademie di tutto il mondo, che riuniscono in sé le migliori persone di scienze e lettere, ed in particolare la nostra storica Accademia dei Lincei, hanno un ruolo importante nel consigliare il mondo politico sulle conseguenze sociali, positive e negative, del presente frenetico sviluppo del commercio, delle comunicazioni, dell’informazione e delle scienze nella società. In questo, la matematica svolge un importante ruolo anche se spesso non è visibile al grande pubblico. Parafrasando il motto di Pasteur sulla scienza, la matematica non è divisa tra matematica astratta e matematica applicata, esiste solo l’applicazione della matematica che deve essere rivolta al bene di tutti.