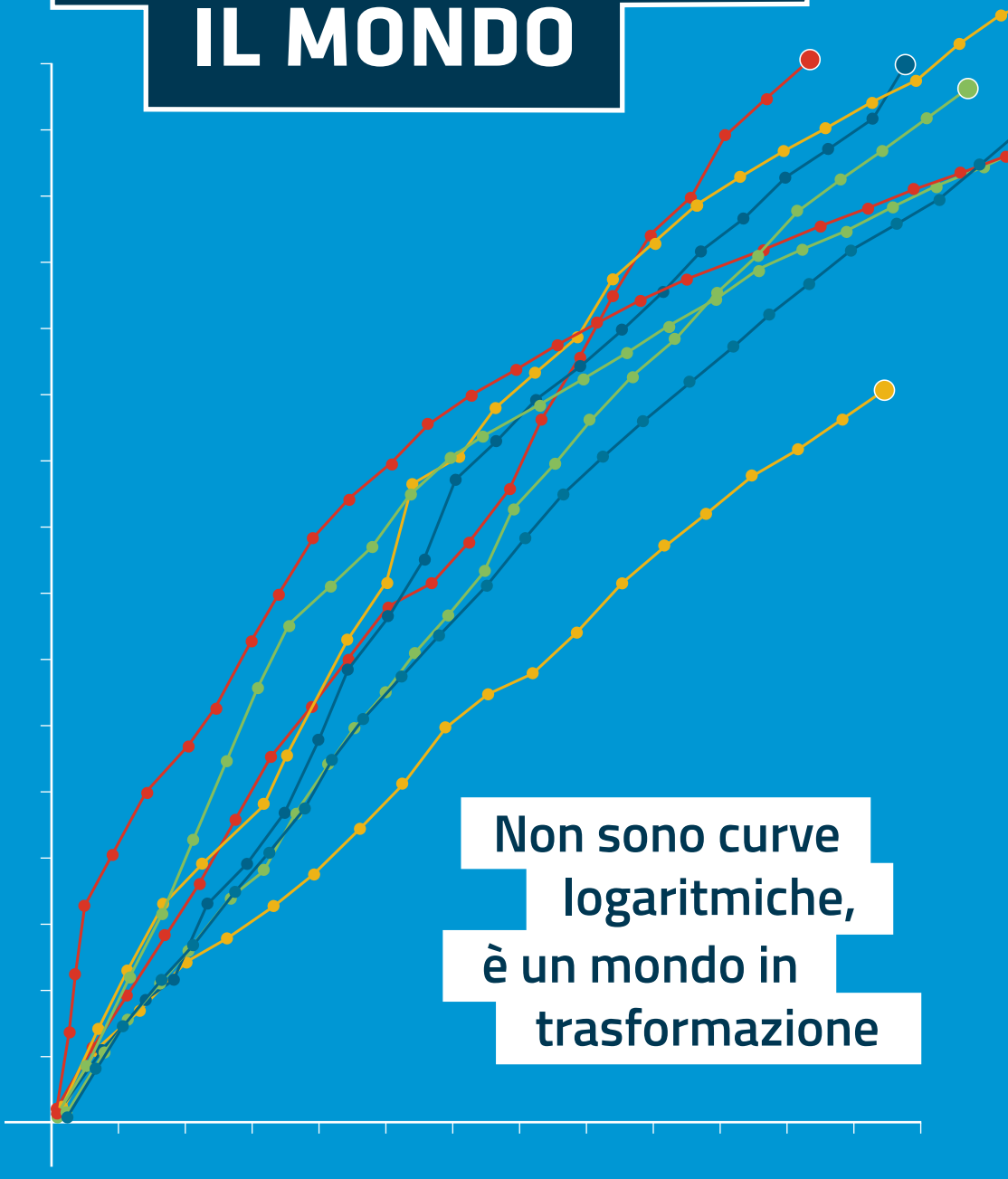
LA MATEMATICA CHE TRASFORMA IL MONDO

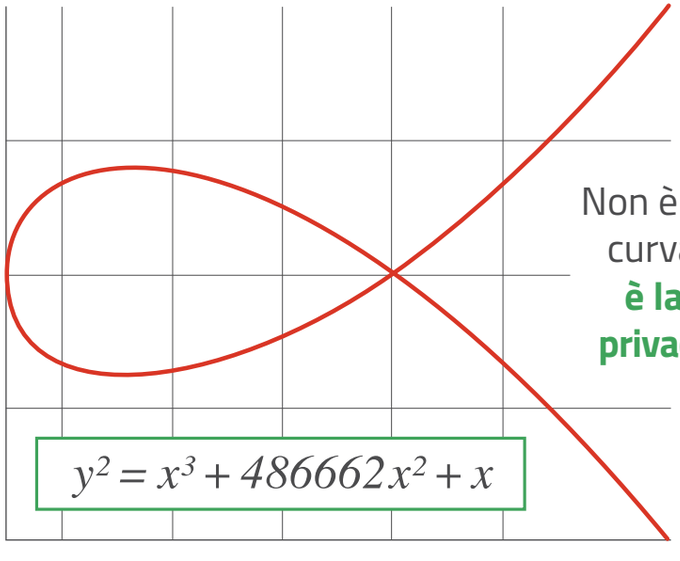


Non sono curve logaritmiche, è un mondo in trasformazione

FORMULE CHE STANNO CAMBIANDO IL PIANETA

I calcoli matematici sono alla base di tutto: **dai big data all'intelligenza artificiale e dai social network alla privacy digitale**, ma anche dei modelli climatici, finanziari o epidemiologici che ci aiutano a comprendere il nostro ambiente. In tutte le aree, **la matematica segna la strada da seguire e anticipa il futuro.**

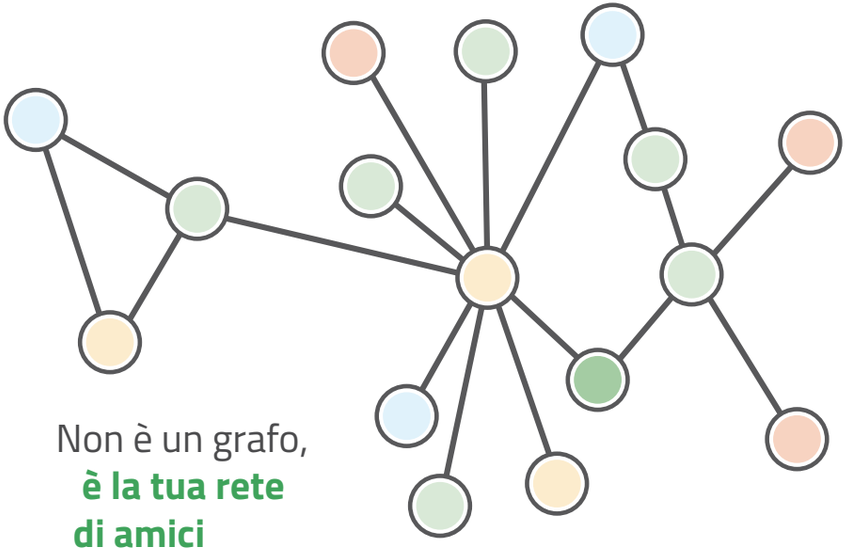
La matematica è passata dalla descrizione del mondo alla sua trasformazione.



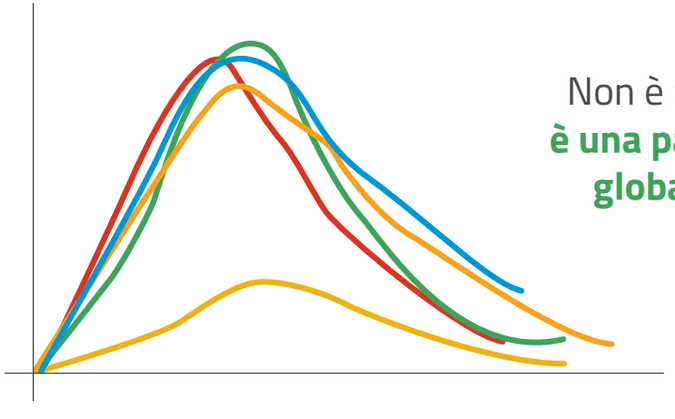
Non è una curva ellittica, **è la nostra privacy digitale**

$$T = \left(\frac{(1-a)\,S}{e\sigma} \right)^{1/4}$$

Non è un'equazione, **è il cambiamento climatico**



Non è un grafo, **è la tua rete di amici**



Non è un grafico, **è una pandemia globale**

UNA COLLEZIONE UNICA E INNOVATIVA

La prima biblioteca di matematica nata dopo la rivoluzione dei dati che sta trasformando il mondo.

Il panorama **più completo**

Big data, criptovalute, social network, modelli climatici: la trattazione di tutte le aree che definiscono il nostro presente.

La matematica **più affascinante**

I teoremi di Fermat e la crittografia, la teoria dei grafi, la geometria non euclidea, la statistica e il *machine learning*: i concetti matematici chiave alla base delle grandi trasformazioni.

Le menti geniali **che muovono il mondo**

Ogni libro presenta un esempio avvincente di come menti geniali della matematica stanno trasformando il mondo: da Spotify a Facebook, passando attraverso Fukushima e la previsione delle crisi future.

RIVOLUZIONARI, AUDACI, RIBELLI... MATEMATICI!

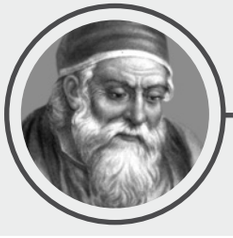
Oggi più che mai, le menti matematiche trasformano il mondo.

Vi sveleremo la prospettiva di coloro che usano la matematica per trasformare il nostro mondo. Un nuovo modo di fare divulgazione che vi avvicinerà **alla matematica in prima persona.**

Nel 1735, **Eulero** risolse "Il problema dei ponti di Königsberg". Fu il seme da cui nacque la teoria dei grafi.

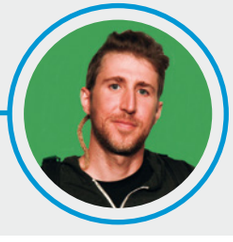
Quasi trecento anni dopo, la prima donna ingegnere nella storia di Facebook, **Ruchi Sanghvi,** applica concetti avanzati di teoria dei grafi per trasformare il modo in cui milioni di utenti utilizzano il social network.

Dopo oltre duemila anni di egemonia, nel XIX secolo fu dimostrato che vi sono altre geometrie oltre a quella di **Euclide.**



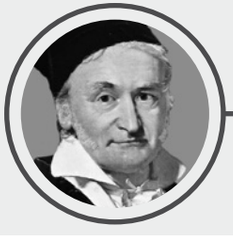
Nel 2011, **i matematici dell'Agenzia Giapponese per l'Energia Atomica** si sono serviti delle geometrie non euclidee per prevedere l'espansione dell'impronta radioattiva di Fukushima e salvare innumerevoli vite.

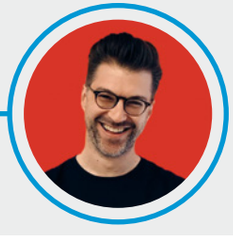
Tra il 1637 e il 1640, **Pierre de Fermat** enunciò i teoremi conosciuti come "Piccolo" e "Ultimo".



Nel 2015, il crittografo **Moxie Marlinspike** si ispira a entrambi i teoremi per progettare un protocollo di crittografia che garantisca la privacy di WhatsApp.

Carl Friedrich Gauss, nel 1801 inventò il metodo dei minimi quadrati per calcolare le orbite.





Matthew Ogle, di Spotify, applica il metodo di Gauss e altre tecniche di *machine learning* e propone un algoritmo che, come per magia, indovina i gusti musicali degli utenti.

LA MATEMATICA NON È MAI STATA COSÌ VIVA

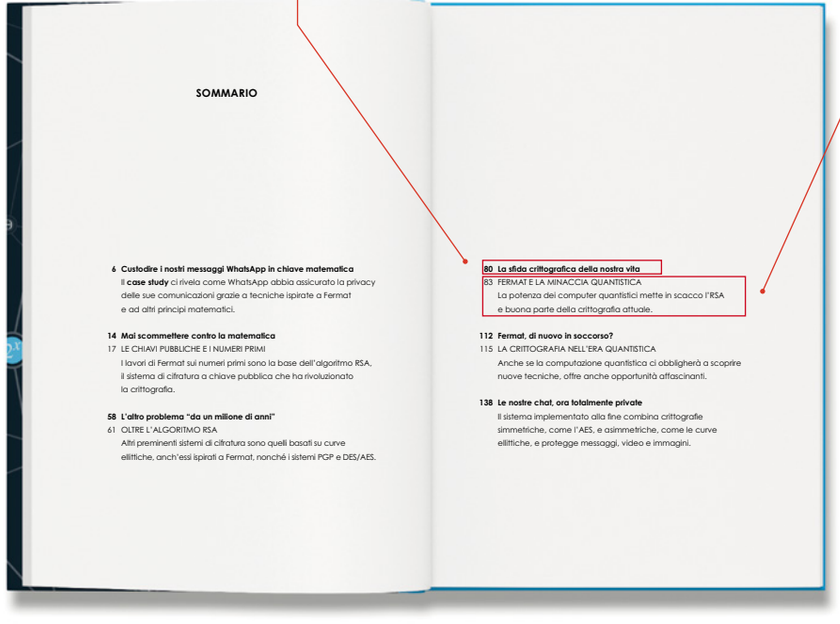
Per la prima volta la matematica e i suoi protagonisti, con tutti gli strumenti per comprenderla.

Da un lato, uno **stile piacevole**, un'**organizzazione chiara** e un'**ampia varietà di elementi grafici**. Dall'altro, attraverso i **case studies** scoprirete come i concetti matematici trattati nel volume **influiscano sulla nostra vita quotidiana**. Storie avvincenti che vi guideranno alla scoperta di **WhatsApp** e **Google**, passando attraverso la **lotta ai cambiamenti climatici** e **la prevenzione delle crisi future**.

Il sommario include sia i capitoli sia gli episodi del case study.

Episodio del **case study**

Capitolo con la sua descrizione



SOMMARIO

6 Custodire i nostri messaggi WhatsApp in chiave matematica
Il **case study** ci rivela come WhatsApp abbia assicurato la privacy delle sue comunicazioni grazie a tecniche ispirate a Fermat e ad altri principi matematici.

14 Mai scommettere contro la matematica
17 LE CHIAVI PUBBLICHE E I NUMERI PRIMI
I lavori di Fermat sui numeri primi sono la base dell'algoritmo RSA, il sistema di cifratura a chiave pubblica che ha rivoluzionato la crittografia.

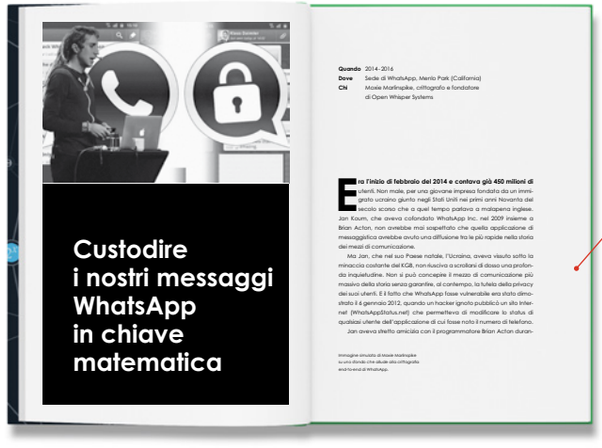
58 L'altro problema "da un milione di anni"
61 OLTRE L'ALGORITMO RSA
Altri preminenti sistemi di cifratura sono quelli basati su curve ellittiche, anch'essi ispirati a Fermat, nonché i sistemi PGP e DES/AES.

80 La sfida crittografica della nostra vita
83 FERMAT E LA MINACCIA QUANTISTICA
La potenza dei computer quantistici mette in scacco l'RSA e buona parte della crittografia attuale.

112 Fermat, di nuovo in soccorso?
115 LA CRITTOGRAFIA NELL'ERA QUANTISTICA
Anche se la computazione quantistica ci obbligherà a scoprire nuove tecniche, offre anche opportunità affascinanti.

138 Le nostre chat, ora totalmente private
Il sistema implementato alla fine combina crittografie simmetriche, come l'AES, e asimmetriche, come le curve ellittiche, e protegge messaggi, video e immagini.

Case study



Custodire i nostri messaggi WhatsApp in chiave matematica

Quando 2014-2016
Dove Sede di WhatsApp, Menlo Park (California)
Chi Moxie Marlinspike, crittografo e fondatore di Open Whisper Systems

Era l'inizio di febbraio del 2014 e contava già 450 milioni di utenti. Non male, per una giovane impresa fondata da un immigrato ucraino giunto negli Stati Uniti nei primi anni Novanta del secolo scorso che a quel tempo parlava a malapena inglese. Jan Koum, che aveva cofondato WhatsApp Inc. nel 2009 insieme a Brian Acton, non avrebbe mai sospettato che quella applicazione di messaggistica avrebbe avuto una diffusione tra le più rapide nella storia dei mezzi di comunicazione.

Ma Jan, che nel suo Paese natale, l'Ucraina, aveva vissuto sotto la minaccia costante del KGB, non riusciva a scrollarsi di dosso una profonda inquietudine. Non si può concepire il mezzo di comunicazione più massivo della storia senza garantire, al contempo, la tutela della privacy dei suoi utenti. E il fatto che WhatsApp fosse vulnerabile era stato dimostrato il 6 gennaio 2012, quando un hacker ignoto pubblicò un sito Internet (WhatsAppStatus.net) che permetteva di modificare lo status di qualsiasi utente dell'applicazione di cui fosse noto il numero di telefono.

Jan aveva stretto amicizia con il programmatore Brian Acton duran-

Immagine simulata di Moxie Marlinspike su uno sfondo che allude alla crittografia end-to-end di WhatsApp.

Il case study **inizia con la presentazione della sfida matematica e dei suoi protagonisti...**

Continua sotto forma di **introduzione a ciascun capitolo...**

Mai scommettere contro la matematica

Fermat lo formulò così: "Se *p* è un numero primo, allora per ogni numero naturale *a*, con *a*>0, *a*^*p* (mod *p*)".

— No, le formule non le leggerà nessuno — pensò.

E riscrisse: "Qualunque numero primo divide una delle potenze meno uno di una qualsiasi progressione geometrica e l'esponente di tale potenza è un divisore del numero primo meno uno".

— Ora sì che ci capisce — disse tra sé, con un sorriso ironico.

Moxie finì per cancellare dal suo blog il post con cui pensava di spiegare il ruolo fondamentale del primo teorema di Fermat nel più diffuso degli algoritmi a chiave pubblica, l'RSA. Dopotutto, lui stesso aveva evitato di includere questo algoritmo tra le primitive del protocollo Signal. Non certo, però, perché mancasse di efficacia o, tanto meno, di bellezza. I matematici erano affascinati dall'RSA perché si avvaleva dei numeri primi, i "pupilli" della matematica pura. Si trattava di un esempio straordinario di come alcune delle idee più astratte della matematica potevano essere applicate alla soluzione di un problema pratico.

Idee matematiche in soccorso a problemi pratici: la crittografia vantava molti altri esempi simili. Nel complesso, la disciplina coniugava aspetti artistici e scientifici, un connubio che senza dubbio contribuiva al suo fascino. La parte scientifica risiedeva in sistemi di cifratura come quelli a sostituzione e trasposizione oppure in strumenti come l'aritmetica modulare o l'analisi delle frequenze. L'alto artistico, quella parte della crittografia che veniva mostrata nei film, risiedeva nella sfida di far giungere in sicurezza al destinatario del messaggio cifrato la chiave che gli avrebbe permesso di decifrarlo. Ed era proprio questo il motivo per cui la crittografia a chiave pubblica, l'idea geniale di Diffie e Hellman, gli sembrava così affascinante. Con il loro schema teorico che descriveva il modo in cui una chiave pubblica avrebbe potuto essere distribuita in maniera sicura, Diffie e Hellman avevano introdotto un'idea astratta capace di fornire una soluzione al principale problema pratico della crittografia. Come Fermat con l'RSA.

Mai scommettere contro la matematica, concluse Moxie. Si perderebbe sicuramente.

15

Le nostre chat, ora totalmente private

Erano trascorsi più di due anni da quando Jan, Brian e Moxie si erano riuniti nel febbraio del 2014, e l'implementazione completa di Signal in tutto WhatsApp era alle sue battute finali. Moxie aveva lasciato agli ingegneri le sue ultime istruzioni e aveva deciso di trascorrere alcuni giorni in mare a bordo del suo catamarano, sicuro di avere ormai raggiunto l'obiettivo finale. Mentre stava per partire, ricevette un messaggio di Signal da Brian Acton che si complimentava per il suo grande lavoro. Gli restituì la cortesia mentre la barca abbandonava lentamente la baia.

Il 5 aprile 2016, Brian e Jan pubblicarono il seguente post sul blog di WhatsApp:

> WhatsApp ha sempre avuto come priorità quella di rendere i dati e la comunicazione il più possibile sicuri. E oggi siamo orgogliosi di annunciare che abbiamo completato una sviluppo tecnologico che rende WhatsApp leader nella protezione della vostra comunicazione privata: la crittografia end-to-end completa. D'ora in poi, quando voi e i vostri contatti utilizzerete l'ultima versione dell'applicazione, ogni chiamata che farete e ogni messaggio, foto, video, file e messaggio vocale che invierete saranno crittografati end-to-end in modo automatico, compresse le chat di gruppo. L'idea è semplice: quando si invia un messaggio, solo la persona o il gruppo verso cui il messaggio è stato inviato può leggerlo. Nessun altro può vedere quel messaggio. Non i cybercriminali. Non gli hacker. Non i regimi oppressivi. Nemmeno noi. La crittografia end-to-end aiuta a rendere la comunicazione via WhatsApp privata. Sostanzialmente è simile a una conversazione faccia a faccia.

Da quel momento in avanti, WhatsApp è diventata una scatola nera, opaca anche per il suo stesso ideatore.

139

E culmina in un **epilogo** che chiude il libro.

Capitoli

$$y = \alpha + \beta x + \varepsilon$$

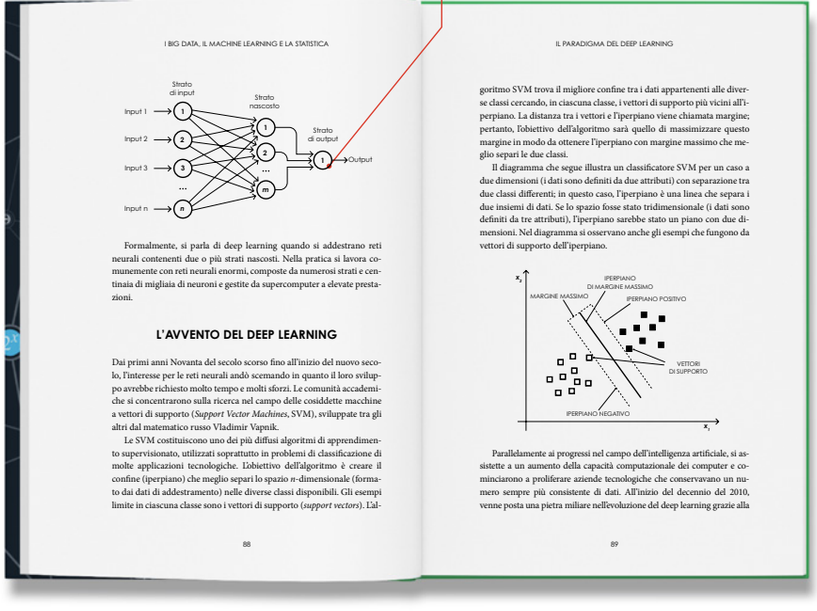
Formula della regressione lineare semplice, dove *y* è la variabile dipendente, *x* la variabile indipendente, *α* e *β* sono i parametri di stima ed *ε* l'errore di stima.

In principio fu la regressione

Il cofondatore dell'azienda statunitense di microprocessori Intel formulò nel 1965 la legge che avrebbe segnato il cammino della rivoluzione digitale. Fin dall'inizio fu battezzata con il suo nome, quello di Gordon E. Moore, un chimico e fisico californiano che aveva elaborato la seguente previsione: il numero di transistor per unità di superficie in un microprocessore, una misura infallibile della sua capacità di calcolo, raddoppia ogni 12 mesi. Dieci anni dopo, lo scienziato si corresse per difetto: la nuova legge di Moore stabiliva che il raddoppio del numero di transistor si sarebbe prodotto ogni 24 mesi, una progressione di crescita che si è avverata per cinque decenni. Questa legge di crescita esponenziale della capacità dei microprocessori si può applicare anche ad altre grandezze dipendenti dalla stessa, come per esempio la capacità di memorizzazione dei dati.

Ovviamente, con il passare del tempo, i termini utilizzati per esprimere la capacità di memorizzazione e il volume di trasmissione dei dati si sono adeguati gradualmente a questo sviluppo inarrestabile: dal bit al byte (8 bit) e al kilobyte (1000 byte), sufficienti per misurare la capacità dei computer della metà del secolo scorso, passando per il megabyte (10^6 byte) e il gigabyte (10^9) fino ad arrivare in tempi più recenti all'imponente terabyte (10^{12}), il cui prefisso "tera" deriva dal greco "mostro". Queste unità di misura sono state superate

Le **notazioni matematiche** essenziali e i numerosi **disegni, grafici e diagrammi** forniscono supporto visivo e aiutano a comprendere i concetti più astratti.



Formalmente, si parla di deep learning quando si addestrano reti neurali contenenti due o più strati nascosti. Nella pratica si lavora comunemente con reti neurali enormi, composte da numerosi strati e centinaia di migliaia di neuroni e gestite da supercomputer a elevate prestazioni.

L'AVVENTO DEL DEEP LEARNING

Dai primi anni Novanta del secolo scorso fino all'inizio del nuovo secolo, l'interesse per le reti neurali andò scemando in quanto il loro sviluppo avrebbe richiesto molto tempo e molti sforzi. Le comunità accademiche si concentrarono sulla ricerca nel campo delle cosiddette macchine a vettori di supporto (*Support Vector Machines*, SVM), sviluppate tra gli altri dal matematico russo Vladimir Vapnik.

Le SVM costituiscono uno dei più diffusi algoritmi di apprendimento supervisionato, utilizzati soprattutto in problemi di classificazione di molte applicazioni tecnologiche. L'obiettivo dell'algoritmo è creare il confine (iperpiano) che meglio separi lo spazio *n*-dimensionale (formato dai dati di addestramento) nelle diverse classi disponibili. Gli esempi limite in ciascuna classe sono i vettori di supporto (*support vectors*). L'al-

goritmo SVM trova il migliore confine tra i dati appartenenti alle diverse classi cercando, in ciascuna classe, i vettori di supporto più vicini all'iperpiano. La distanza tra i vettori e l'iperpiano viene chiamata margine; pertanto, l'obiettivo dell'algoritmo sarà quello di massimizzare questo margine in modo da ottenere l'iperpiano con margine massimo che meglio separi le due classi.

Il diagramma che segue illustra un classificatore SVM per un caso a due dimensioni (i dati sono definiti da due attributi) con separazione tra due classi differenti; in questo caso, l'iperpiano è una linea che separa i due insiemi di dati. Se lo spazio fosse stato tridimensionale (i dati sono definiti da tre attributi), l'iperpiano sarebbe stato un piano con due dimensioni. Nel diagramma si osservano anche gli esempi che fungono da vettori di supporto dell'iperpiano.

Parallelamente ai progressi nel campo dell'intelligenza artificiale, si assistette a un aumento della capacità computazionale dei computer e cominciarono a proliferare aziende tecnologiche che conservavano un numero sempre più consistente di dati. All'inizio del decennio del 2010, venne posta una pietra miliare nell'evoluzione del deep learning grazie alla

ma coordinata o ascissa del punto e indica la distanza a cui si trova tale punto rispetto all'asse verticale; la "*y*" è la seconda coordinata o ordinata del punto e indica la distanza a cui si trova il punto dall'asse orizzontale.

Ebbene, una curva ellittica è l'insieme dei punti del piano le cui coordinate (x,y) soddisfano l'equazione $y^2 = x^3 + ax + b$ per qualsiasi valore fisso di *a* e *b* (inoltre, per ragioni tecniche, si richiede che $4a^3 + 27b^2 \neq 0$). La figura seguente mostra esempi di varie curve ellittiche per diversi valori di *a* e *b*.

Esempi di curve ellittiche in un sistema di coordinate cartesiane; si può apprezzare la loro simmetria rispetto all'asse delle ascisse.

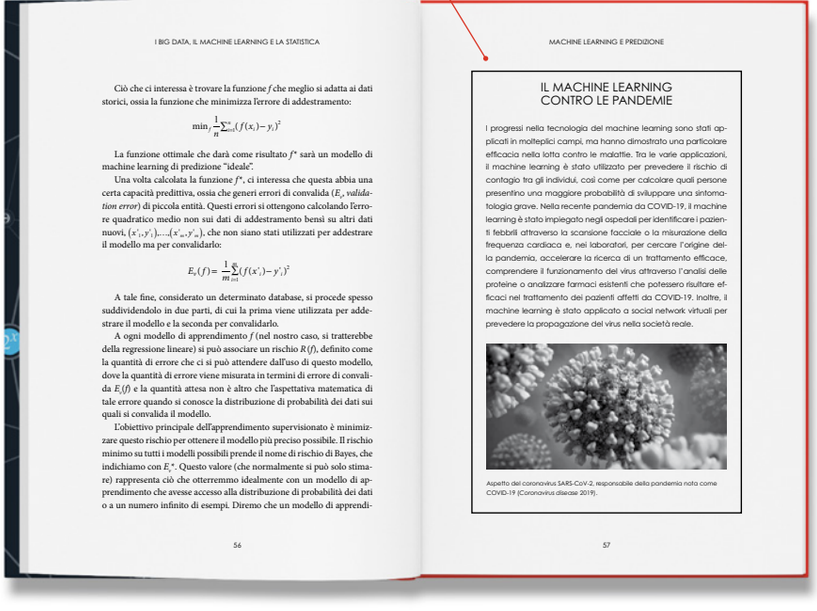
Curve rilevanti in crittografia sono la curva 25519, utilizzata nel protocollo Signal, la cui equazione è $y^2 = x^3 + 486662x^2 + x$, e la curva secp256k1, utilizzata nella maggior parte delle criptovalute, come il Bitcoin, l'Ethereum e molte altre. La curva secp256k1 è definita dall'equazione $y^2 = x^3 + 7$ ed è raffigurata nella figura seguente:

FERMAT E IL SEGRETO DELLE CURVE

Andrew Wiles.

Dopo ben 358 anni, il teorema più famoso della storia, formulato da Pierre de Fermat nel 1637, è stato finalmente dimostrato, grazie al britannico Andrew Wiles. "Se *n* è un numero intero maggiore di 2, allora non esistono tre numeri naturali *x*, *y*, *z* tali per cui sia soddisfatta l'uguaglianza $x^n + y^n = z^n$". Un enunciato tanto semplice da poter sembrare persino banale, ma che dal XVII secolo ha fatto arrovellare i cervelli dei più illustri matematici. Per la sua risoluzione, Wiles, che conosceva il teorema già a 10 anni, si basò sulla congettura di Taniyama-Shimura-Weil e sulla relazione che il matematico statunitense Kenneth A. Ribet stabilì tra questa congettura e l'ultimo teorema di Fermat. Se fosse stato possibile dimostrare che questo teorema era un caso particolare della congettura, corrispondente alle curve ellittiche (un campo che Wiles aveva già studiato), ciò avrebbe condotto direttamente alla sua dimostrazione. Wiles dedicò sette anni alla ricerca dell'anelata dimostrazione finché, nel 1993, credette di aver dimostrato il teorema. Tuttavia, la revisione del suo articolo rivelò un errore, che riuscì a correggere dopo altri due anni di duro lavoro. Oltre ad aver realizzato il suo sogno dell'infanzia e aver raggiunto la fama mondiale che da allora lo accompagna, Wiles ha ricevuto vari premi e onorificenze, tra cui, nel 2016, il premio Abel, definito il "Nobel" della matematica.

I **box** completano e arricchiscono il testo principale. Vi faranno scoprire la vita di grandi matematici e vi mostreranno campi sorprendenti in cui la matematica trova applicazione.



Ciò che ci interessa è trovare la funzione *f* che meglio si adatta ai dati storici, ossia la funzione che minimizza l'errore di addestramento:

$$\min_f \frac{1}{n} \sum_{i=1}^{n} (f(x_i) - y_i)^2$$

La funzione ottimale che darà come risultato f^* sarà un modello di machine learning di predizione "ideale".

Una volta calcolata la funzione f^*, ci interessa che questa abbia una certa capacità predittiva, ossia che generi errori di convalida (E_v, *validation error*) di piccola entità. Questi errori si ottengono calcolando l'errore quadratico medio non sui dati di addestramento bensì su altri dati nuovi, $(x'_1, y'_1), \ldots, (x'_m, y'_m)$, che non siano stati utilizzati per addestrare il modello ma per convalidarlo:

$$E_v(f) = \frac{1}{m} \sum_{i=1}^{m} (f(x'_i) - y'_i)^2$$

A tale fine, considerato un determinato database, si procede spesso suddividendolo in due parti, di cui la prima viene utilizzata per addestrare il modello e la seconda per convalidarlo.

A ogni modello di apprendimento *f* (nel nostro caso, si tratterebbe della regressione lineare) si può associare un rischio $R(f)$, definito come la quantità di errore che ci si può attendere dall'uso di questo modello, dove la quantità di errore viene misurata in termini di errore di convalida $E_v(f)$ e la quantità attesa non è altro che l'aspettativa matematica di tale errore quando si conosce la distribuzione di probabilità dei dati sui quali si convalida il modello.

L'obiettivo principale dell'apprendimento supervisionato è minimizzare questo rischio per ottenere il modello più preciso possibile. Il rischio minimo su tutti i modelli possibili prende il nome di rischio di Bayes, che indichiamo con E_*. Questo valore (che normalmente si può solo stimare) rappresenta ciò che otterremmo idealmente con un modello di apprendimento che avesse accesso alla distribuzione di probabilità dei dati o a un numero infinito di esempi. Diremo che un modello di apprendi-

IL MACHINE LEARNING CONTRO LE PANDEMIE

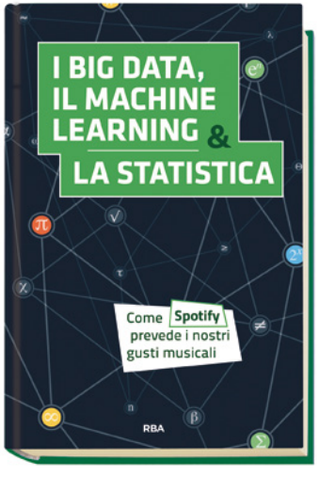
I progressi nella tecnologia del machine learning sono stati applicati in molteplici campi, ma hanno dimostrato una particolare efficacia nella lotta contro le malattie. Tra le varie applicazioni, il machine learning è stato utilizzato per prevedere il rischio di contagio tra gli individui, così come per calcolare quali persone presentino una maggiore probabilità di sviluppare una sintomatologia grave. Nella recente pandemia da COVID-19, il machine learning è stato impiegato negli ospedali per identificare i pazienti febbrili attraverso la scansione facciale o la misurazione della frequenza cardiaca e, nei laboratori, per cercare l'origine della pandemia, accelerare la ricerca di un trattamento efficace, comprendere il funzionamento del virus attraverso l'analisi delle proteine o analizzare farmaci esistenti che potessero risultare efficaci nel trattamento dei pazienti affetti da COVID-19. Inoltre, il machine learning è stato applicato a social network virtuali per prevedere la propagazione del virus nella società reale.

Aspetto del coronavirus SARS-CoV-2, responsabile della pandemia nota come COVID-19 (Coronavirus disease 2019).

I PRIMI TITOLI DELLA COLLANA

Il cosiddetto "piccolo teorema" di Fermat, che riguarda alcune proprietà dei numeri primi, è un elemento chiave dell'algoritmo RSA, il sistema di cifratura più utilizzato in Internet. Oggi, la sua validità e quella di altri sistemi alternativi, come il sistema basato sulle curve ellittiche, anch'esse correlate a Fermat, sono minacciate dallo sviluppo della computazione quantistica. Tuttavia, stanno già emergendo nuove e affascinanti applicazioni matematiche che garantiranno la nostra privacy in un futuro post-quantistico.

Un crittografo geniale, Moxie Marlinspike, ideò Signal, uno dei protocolli di crittografia più completi, e lo applicò a WhatsApp per assicurare la cifratura end-to-end di tutti i suoi contenuti.



I big data hanno comportato un'autentica rivoluzione scientifica e concettuale. Applicati a molti ambiti, dal clima al comportamento umano, i modelli matematici alimentati dai dati si sono dimostrati in grado di fare previsioni molto precise. Alla base di questa nuova era c'è il machine learning, che a sua volta trova il proprio fondamento nella statistica e include concetti estremamente affascinanti, come il deep learning, un tentativo di replicare il modo in cui il cervello umano tratta grandi quantità di informazioni in tempo reale.

Come fa Spotify a indovinare i nostri gusti musicali quando ci presenta una playlist? La risposta a questa domanda risiede nell'applicazione Discover Weekly, sviluppata grazie ai big data.

Quanti gradi di separazione esistono tra gli utenti di Facebook? Come riconoscere gli influencer su Instagram? Come si propagano le notizie virali su Twitter? La teoria dei grafi, una disciplina matematica nata quasi tre secoli fa, cerca di rispondere a queste domande nonché di studiare e comprendere la formazione delle moderne reti sociali e la loro evoluzione. Un grafo è una struttura formata da un minimo numero di elementi (nodi connessi da archi), ed è in grado di rappresentare le reti più complesse.

I fondamenti matematici su cui si fonda l'algoritmo chiave di Facebook, lo scenario dove interagiscono miliardi di persone in tutto il mondo, realizzato per mano di una dei suoi promotori: Ruchi Sanghvi.

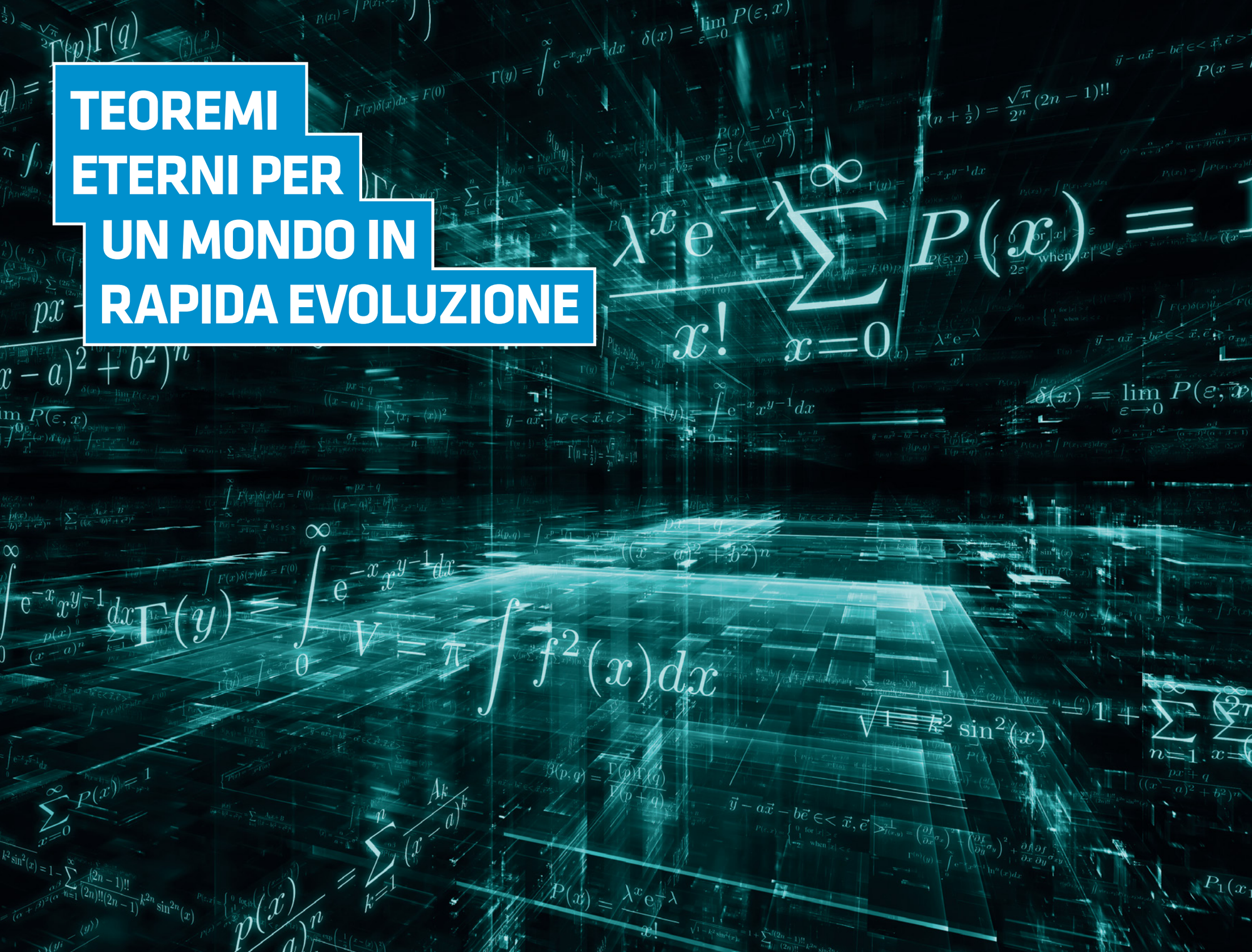
Le mappe digitali sono diventate uno strumento abituale nella vita quotidiana: le utilizziamo per orientarci quando viaggiamo, per cercare i ristoranti più vicini a casa e per conoscere i punti del nostro itinerario in cui troveremo traffico... La disponibilità di sistemi di cartografia e geolocalizzazione così versatili e potenti non sarebbe possibile senza le geometrie non euclidee, nate dalla volontà di rappresentare su un piano la superficie terrestre, con tutta la sua complessità.

Alcuni ricercatori giapponesi riuscirono a determinare, con l'ausilio della matematica, la dispersione della contaminazione radioattiva dopo l'incidente dell'impianto nucleare di Fukushima.

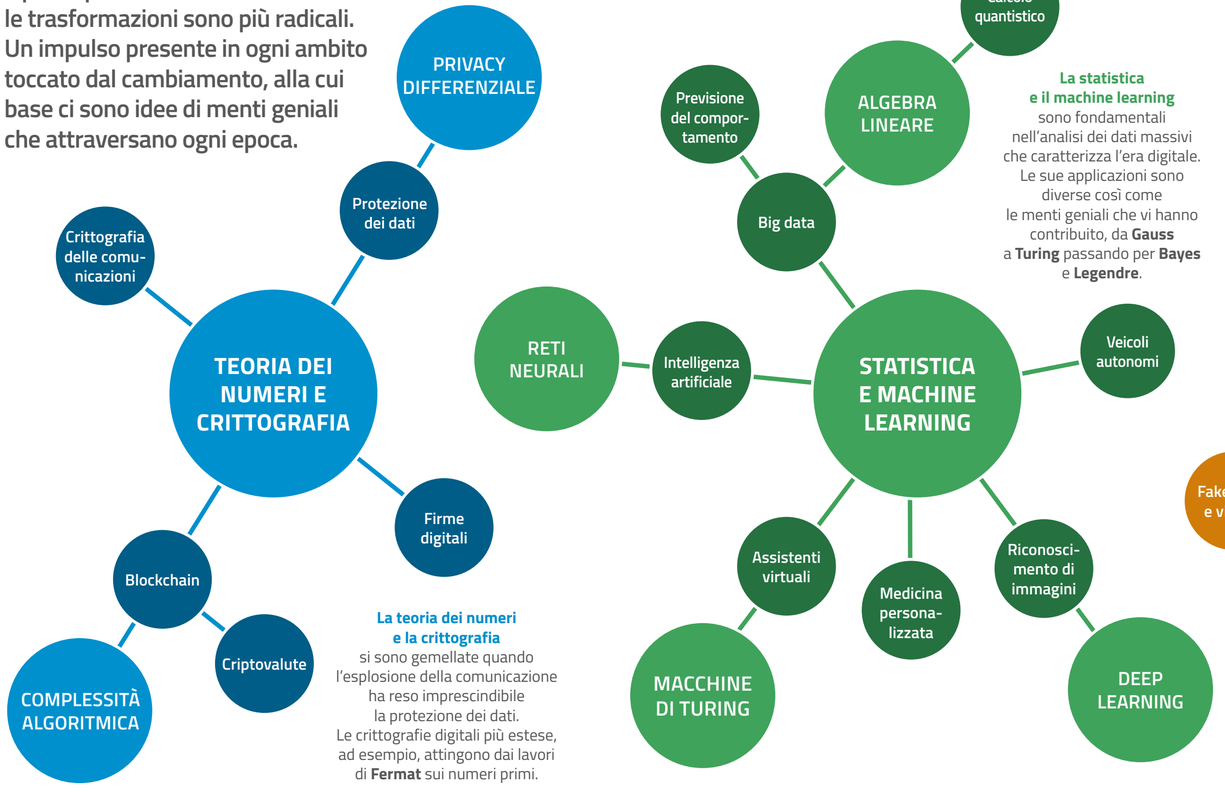
Lo sviluppo dell'intelligenza artificiale mira a far sì che le macchine possano apprendere da sole, trovino soluzioni ottimali a problemi complessi e riescano a fare deduzioni corrette in maniera autonoma. L'obiettivo, in definitiva, è costruire menti sintetiche che ragionino. Quali algoritmi racchiudono queste macchine pensanti? Qual è la matematica che dà vita alla magia del ragionamento artificiale? Come sono queste reti neurali di apprendimento profondo che riproducono il funzionamento del cervello umano?

L'essere umano contro l'intelligenza artificiale Watson sviluppata da IBM: il racconto del tentativo di rottura della barriera di Alan Turing al quiz televisivo *Jeopardy*!

TEOREMI ETERNI PER UN MONDO IN RAPIDA EVOLUZIONE



Il ruolo della matematica è più importante laddove le trasformazioni sono più radicali. Un impulso presente in ogni ambito toccato dal cambiamento, alla cui base ci sono idee di menti geniali che attraversano ogni epoca.



La teoria dei numeri e la crittografia si sono gemellate quando l'esplosione della comunicazione ha reso imprescindibile la protezione dei dati. Le crittografie digitali più estese, ad esempio, attingono dai lavori di **Fermat** sui numeri primi.

La statistica e il machine learning sono fondamentali nell'analisi dei dati massivi che caratterizza l'era digitale. Le sue applicazioni sono diverse così come le menti geniali che vi hanno contribuito, da **Gauss** a **Turing** passando per **Bayes** e **Legendre**.

La teoria dei grafi, che studia le relazioni tra oggetti, si è rivelata fondamentale per comprendere un mondo in cui l'interconnessione è la norma. Non lo immaginava il suo ideatore, **Eulero**, che la considerava un divertimento.

Le equazioni differenziali descrivono il carattere variabile della natura in termini matematici, e sono alla base dei modelli che tentano di spiegare il mondo fisico. **Newton**, **Leibniz**, **Lagrange** e **Fourier** sono alcuni dei loro padri teorici.

ALTRI TITOLI

La realtà virtuale & la matematica della visione e del movimento
Le criptovalute, la blockchain & la complessità algoritmica
Le previsioni economiche & la curva di Gauss
Gli assistenti virtuali & le macchine di Turing
La protezione dei dati & la privacy differenziale
Le città intelligenti & la teoria delle reti
La predizione del comportamento, le matrici & le regressioni
La formula matematica che rende possibile la comunicazione digitale
L'informatica quantistica & gli spazi vettoriali
La struttura nascosta della rete & le catene di Markov
Le pandemie & le equazioni differenziali
I veicoli autonomi & i loro schemi matematici
I conflitti internazionali & la teoria dei giochi
La prevenzione della guerra cibernetica & la casualità matematica
La nanotecnologia & la matematica
La cyber sorveglianza & i grafi aleatori
L'anticipazione delle catastrofi naturali & l'errore in matematica
I cambiamenti climatici & la matematica del caos
Le strategie politiche & la matematica delle decisioni
Il genoma, le combinazioni & i nodi matematici
L'economia globale & l'ottimizzazione matematica
L'automazione del lavoro & i suoi algoritmi
La medicina personalizzata & la statistica avanzata
I mercati finanziari & l'equazione di Black-Scholes
...

*La collezione è composta da 35 uscite. Prezzo della prima uscita € 2,99. Prezzo della seconda uscita € 9,99. Dalla terza uscita e per tutte le successive prezzo € 9,99 (salvo variazioni dell'aliquota fiscale). L'Editore si riserva il diritto di variare la sequenza delle uscite dell'opera e/o i prodotti allegati. Qualsiasi variazione sarà comunicata nel rispetto delle norme vigenti previste dal codice del consumo (D.lgs 206/2005).
© 2020 RBA ITALIA S.r.l.

RBA

www.matematicarba.it