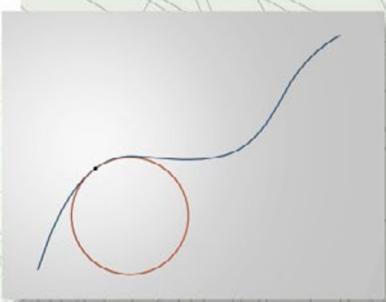
Matematiche ESEMPLARI

Dal compasso ALL'UNIVERSO CURVO

Misurare la forma del mondo in cui viviamo

La curvatura di una linea piana

Come si può misurare la *curvatura* di una linea curva piana in un punto? Un'idea classica è: tra tutte le circonferenze tangenti alla curva in quel punto, il calcolo infinitesimale permette di determinarne una che l'approssima meglio. Se R è il raggio di quella circonferenza, la curvatura della linea in quel punto è, per definizione, 1/R.
Più piccolo è R, più la linea sta curvandosi bruscamente (curvatura grande); più grande è R, minore è la curvatura della linea.
Per una retta la curvatura è nulla.



Dalle curve alle superfici

Carl Friedrich Gauss
(1777-1855)

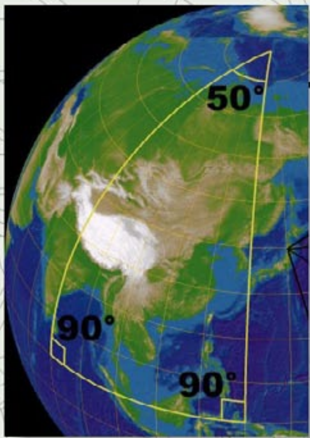
Consideriamo ora una superficie nello spazio. Si può definire un concetto analogo di curvatura? La situazione è più complessa, ma si può fare così. In un punto, consideriamo la retta perpendicolare alla superficie, e tutti i piani che contengono tale retta; ogni piano interseca la superficie lungo una curva, di cui sappiamo misurare la curvatura. Diamo anche un *segno* a questa curvatura, considerandola positiva o negativa a seconda che la curva stia sopra o sotto il piano tangente. Avremo infinite curvature, una per ogni direzione; in particolare, ce ne sarà una massima e una minima: il loro prodotto prende il nome di *curvatura Gaussiana* della superficie in quel punto. Per esempio, la sfera di raggio R ha curvatura gaussiana $1/R^2$. La *pseudosfera* è una superficie di curvatura costante negativa. Un piano o un cilindro hanno curvatura nulla.

Matematiche ESEMPLARI

Dal compasso ALL'UNIVERSO CURVO

La Geometria dell'universo

Gauss ha dimostrato che **la curvatura gaussiana di una superficie può essere calcolata a partire da misurazioni (angoli, distanze) fatte stando sulla superficie stessa,** senza necessità di vederla immersa nello spazio. Nasce così l'idea di "geometria intrinseca".

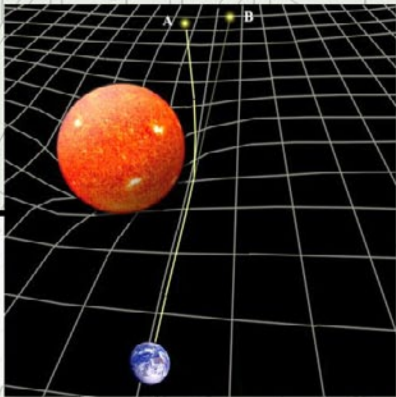


Chi vive sulla superficie di una sfera può accorgersi che il suo "mondo" è curvo anziché piatto, senza bisogno di guardarlo dal di fuori. Per esempio, la somma degli angoli interni di un triangolo disegnato sulla sfera, è *maggiore* di 180°.

Riemann, allievo di Gauss, ha superato il maestro: ha compreso le prospettive sconfinate aperte dalla geometria intrinseca e creato una geometria degli "spazi curvi" (detti "varietà"), in cui le superfici possono essere definite direttamente, senza far riferimento a uno spazio che le contiene. Tutto è scritto nella "metrica", cioè nel modo in cui si calcolano le distanze tra due punti.In particolare, il nostro universo si può vedere come una "varietà" e possiamo chiederci se esso sia "piatto" o "curvo".

Einstein, nella sua teoria generale della relatività (1916), ha ipotizzato che l'universo sia una **varietà curva**, la cui metrica dipende dalla distribuzione di materia nell'universo: la materia "incurva" lo spazio (più precisamente, lo *spazio-tempo*).

Bernhard Riemann (1826-1866)



Le previsioni di Einstein furono clamorosamente confermate dal fenomeno della deflessione dei raggi luminosi, osservato per la prima volta nel 1919 in occasione di un'eclisse di sole.

Il desiderio di comprendere le proprietà degli oggetti matematici e il loro perché, senza aver paura dell'astrazione, ci ripaga con un'inaspettata e più profonda comprensione del mondo fisico in cui viviamo.

Matematiche ESEMPLARI

La matematica DELLA MUSICA

L'armonia delle frazioni

Il **monocorde** è il semplicissimo strumento musicale su cui Pitagora e i suoi seguaci fecero i primi esperimenti sulle relazioni tra matematica e musica. Si tratta di una corda tesa tra due estremi fissi; sotto la corda scorre un capotasto mobile, che consente di accorciare a piacimento la lunghezza effettiva della corda vibrante.
I pitagorici scoprirono che **l'intervallo tra due note emesse è gradevole a udirsi quando le lunghezze delle corde stanno tra loro in un rapporto semplice.**

Pitagora in un'illustrazione dell'opera *Theorica Musicae di Gafurius*, 1492.

Con linguaggio musicale attuale

RAPPORTO TRA LE LUNGHEZZE DELLE CORDE	INTERVALLO MUSICALE	ESEMPIO
1/2	ottava	do-do
2/3	quinta	do-sol
3/4	quarta	do-fa

Si tratta di intervalli gradevoli al nostro orecchio, che corrispondono a frazioni "semplici". Se invece il rapporto tra le lunghezze fosse 7/17, otterremmo un suono "sgradevole".

Marin Mersenne (1588-1649) compie ***la prima misurazione di una frequenza musicale nel 1648.***

Nel XVII sec. si capisce più profondamente la relazione tra suono emesso e vibrazione della corda: la nota dipende da quante volte al secondo la corda compie un'oscillazione completa, ossia dalla **frequenza della vibrazione**. Ad esempio, la frequenza di 528 vibrazioni al secondo (528 Hertz) produce una nota di *do*.
Più alta è la frequenza, più acuta è la nota.

Il rapporto tra le lunghezze delle corde è uguale al reciproco del rapporto tra le frequenze dei suoni emessi.

Matematiche ESEMPLARI

La matematica DELLA MUSICA

Il punto di vista dell'analisi matematica

Il fenomeno fisico delle vibrazioni di una corda tesa viene studiato matematicamente a partire dalla metà del XVIII sec., con D'Alembert; grandi progressi vengono fatti poi da **Fourier**, intorno al 1830.

L'idea fondamentale di Fourier è che **ogni vibrazione di una corda fissata agli estremi, per quanto complessa, si può vedere come sovrapposizione di tante vibrazioni semplici** (dette "armoniche fondamentali"), di frequenze f, $2f$, $3f$, $4f$, ecc.

Viceversa, quando si suonano contemporaneamente più note *le cui frequenze hanno tra loro rapporti semplici* (ad esempio, le frequenze di *do*, *mi*, *sol* di una stessa ottava stanno tra loro come 1, 5/4, 3/2), il suono risultante è una vibrazione più complessa ma ancora *periodica* e viene percepita dal nostro orecchio come gradevole.

Jean Baptiste Le Rond D'Alembert (1717-1783)

Il modello matematico delle vibrazioni di una corda tesa è costituito da *un'equazione differenziale a derivate parziali (detta appunto equazione della corda vibrante)*.

$$\frac{\partial^2 u(t,x)}{\partial t^2} = c^2 \frac{\partial^2 u(t,x)}{\partial x^2}$$

Equazione della corda vibrante

Jean Baptiste Joseph Fourier (1768-1830)

L'analisi delle frequenze aiuta quindi a comprendere più profondamente quella "armonia dei numeri" che già affascinava Pitagora.

CRITTOGRAFIA

Il cifrario di Cesare

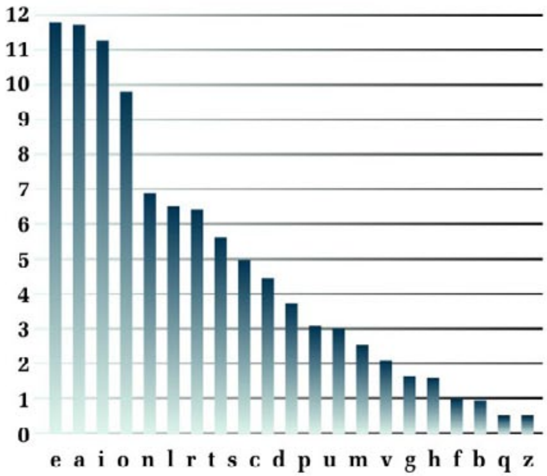
Svetonio riporta l'abitudine di Cesare di criptare le sue corrispondenze riservate sostituendo ogni lettera con quella che la segue di tre posti nell'alfabeto:

$$\mathbf{A} \rightarrow \mathbf{D}, \quad \mathbf{B} \rightarrow \mathbf{E}, \quad \mathbf{C} \rightarrow \mathbf{F}, \quad \mathbf{D} \rightarrow \mathbf{G}, \quad \ldots \quad \mathbf{Z} \rightarrow \mathbf{C}$$

Il Cifrario di Cesare contiene già i due elementi tipici di un codice di crittografia: l'**algoritmo** e la **chiave**. Il primo è la regola (es. spostare in avanti le lettere) la seconda è il parametro (es. 3, cioè il numero dei passi).

Ci sono pochi modi di spostare in avanti le lettere e non è difficile decriptare un messaggio. È meglio sostituire le lettere in un modo apparentemente casuale, ma anche questo sistema, inventato in India, divenne inutile quando gli arabi usarono la statistica, analizzando le frequenze delle lettere dell'alfabeto. Ad esempio, in italiano le lettere più comuni sono nell'ordine E, A, I, O, N, [...].

Giulio Cesare



La tabella mostra una stima della frequenza con cui le lettere dell'alfabeto compaiono in un testo scritto in italiano; le vocali *a*, *e* si presentano con la frequenza di quasi il 12%.

CRITTOGRAFIA

Da Enigma ad oggi

Nel XX secolo la crittografia dovette evolversi in fretta, poiché era diventato facile sia trasmettere i messaggi, sia intercettarli. Nel 1914 i russi subirono a Tannenberg una sconfitta decisiva anche perché i loro messaggi viaggiavano per radio "in chiaro"!
Dopo la prima guerra mondiale i tedeschi crearono la più famosa macchina crittografica della storia, **Enigma**: un apparecchio elettromeccanico nel quale la regola di sostituzione delle lettere cambiava continuamente. I polacchi furono i primi a studiarla e, per la prima volta nella storia della crittografia, non si rivolsero ai linguisti, ma a un gruppo di matematici; fu uno di loro, **Marian Rejewski**, a conseguire i primi successi.

Il monumento a Marian Rejewski (1905-1980) a Bydgoszcz, Polonia, lo ritrae a fianco di "enigma".

Enigma

Il suo lavoro fu proseguito dagli inglesi, grazie al genio di **Alan Turing**, che spezzò il procedimento di Enigma in problemi più semplici e creò una macchina in grado di decriptare i messaggi fin dall'inizio del 1940.

Alan Turing (1912-1954)

La crittografia nell'era di internet

Negli ultimi decenni i crittografi hanno iniziato a usare anche sistemi basati su *due chiavi*: una **chiave pubblica**, che tutti conoscono e con cui chiunque può inviare un messaggio criptato, e una **chiave privata**, che solo il destinatario conosce e gli permette di decriptare il messaggio. Il più famoso dei sistemi a chiave pubblica fu proposto nel 1978 da R. Rivest, A. Shamir e L. Adleman e prende dalle loro iniziali il nome di **sistema RSA**. La sicurezza dei segreti militari, industriali o bancari (come i pagamenti attraverso carte di credito) si basa oggi su sistemi come questo.

CRITTOGRAFIA

La sicurezza dai numeri primi

Da che cosa dipende la sicurezza del sistema RSA? Chi crea le due chiavi sceglie **due numeri primi p, q** (cioè numeri divisibili solo per se stessi e per 1, come sono 2, 3, 5, 7, 11, 13, 17…); **p e q devono essere diversi tra loro e *grandi*** (numeri di circa 100 cifre).
Si calcola il prodotto $n=pq$. A partire da p e q, con una certa regola (che sfrutta un teorema sui numeri primi dovuto a Fermat -17° sec.- e Eulero -18° sec.-) **si determinano altri due interi d, h. Ora la chiave pubblica è la coppia di numeri n e h, mentre la chiave privata è il numero d.**
Conoscendo solo la chiave pubblica, per calcolare d occorrerebbe conoscere p e q, cioè **occorrerebbe saper scomporre il numero n nel prodotto dei due fattori primi che lo compongono**. **Quest'operazione**, banale quando il numero n è "abbastanza piccolo" (basta provare a dividere successivamente n per gli interi 2, 3, 5,…) **richiede un tempo proibitivo quando p e q sono così grandi. Su questo si basa la sicurezza del sistema RSA.**

R. Rivest,
A. Shamir
L. Adleman

1. Scrittura
Chiave pubblica:
$n = 5141$; $h = 17$

2. Codifica e invio

3. Decodifica
Chiave privata:
$d = 881$

d si può calcolare conoscendo $p=53$ e $q=97$, cioè i due fattori in cui si scompone n: $5141 = 53 \times 97$

Così la *teoria dei numeri*, da sempre considerata l'emblema della "matematica pura" e spesso studiata a prescindere da possibili applicazioni, si rivela oggi estremamente utile.

Galleria STORICA

"Senza i concetti, metodi e risultati scoperti e sviluppati dalle generazioni precedenti fino all'antica Grecia non si possono capire né gli scopi né i traguardi della matematica degli ultimi 50 anni".

Hermann Weyl, 1950

Raffaello,
La Scuola di Atene (1511).
Nei tondi Pitagora e Euclide

Raffaello, *La Scuola di Atene (1511)*. Nei tondi Pitagora e Euclide

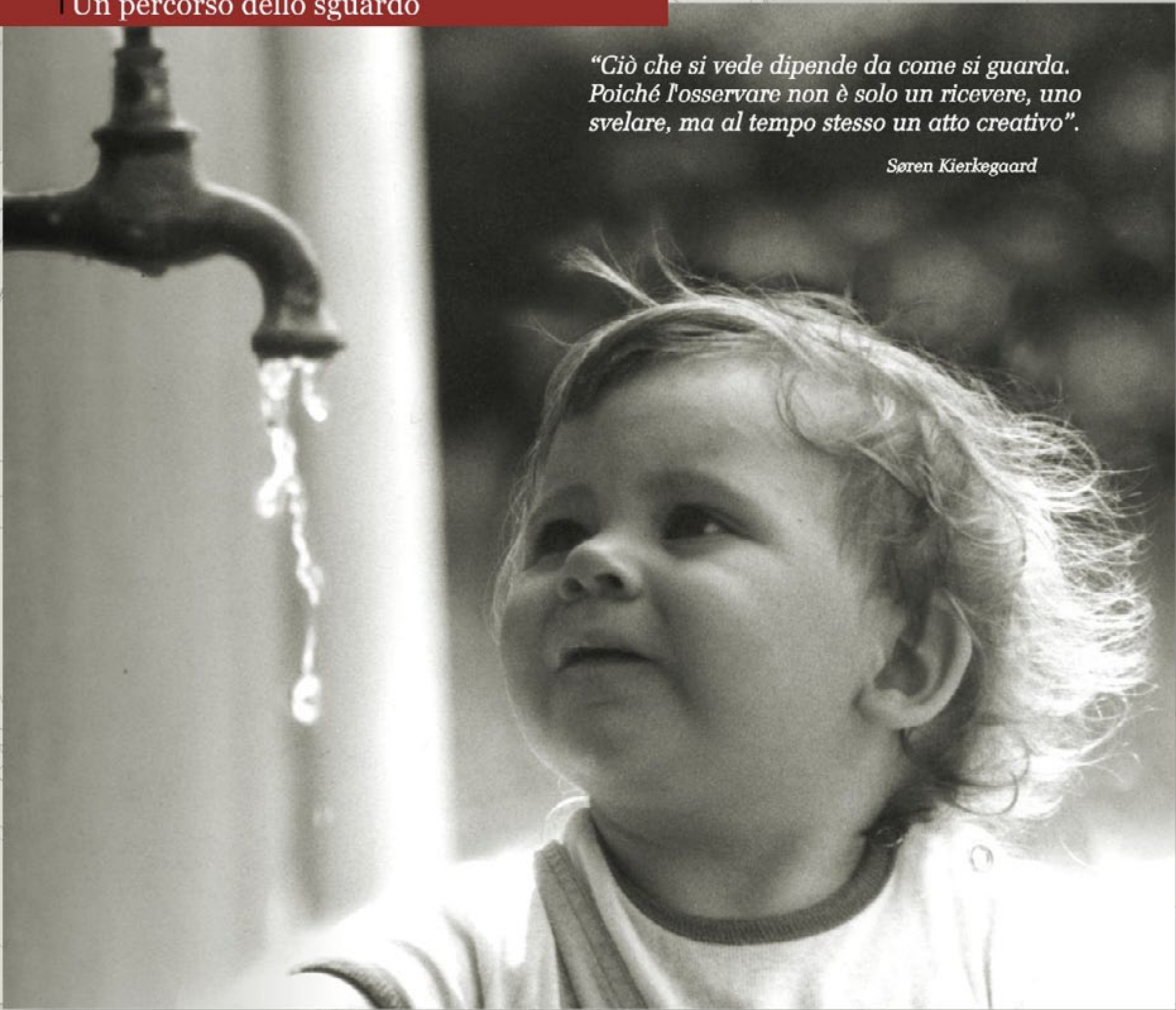
"Senza i concetti, metodi e risultati scoperti e sviluppati dalle generazioni precedenti fino all'antica Grecia non si possono capire né gli scopi né i traguardi della matematica degli ultimi 50 anni".

Hermann Weyl, 1950

La matematica come sapere organizzato emerge e si affina nella civiltà greca tra il 600 a.C. circa (Talete, Pitagora) e il 300 a.C. (Euclide), contemporaneamente al grande pensiero filosofico greco.

La DIMOSTRAZIONE

Un percorso dello sguardo



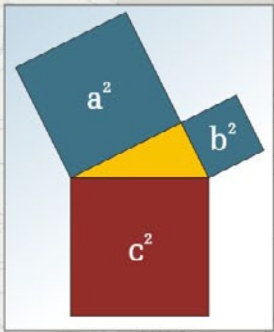
Il TEOREMA

Dove sorge?

Certo il nome di Pitagora è legato al famoso teorema.

$$a^2+b^2=c^2$$

In un triangolo rettangolo il quadrato costruito sull'ipotenusa è equivalente alla somma dei quadrati costruiti sui cateti.



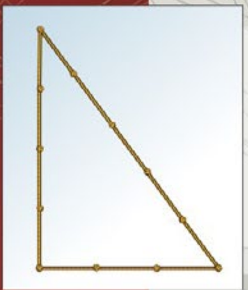
"Avevo 12 anni quando un mio vecchio zio mi enunciò il teorema di Pitagora e dopo molti sforzi riuscii a dimostrarlo. È stata un'esperienza meravigliosa scoprire come l'uomo sia in grado di raggiungere un tale livello di certezza e di chiarezza nel puro pensiero. E sono stati i Greci per primi ad indicarcene la possibilità, con la geometria".

Albert Einstein

Si racconta che la relazione fosse già nota nell'antico Egitto ma non è documentato, mentre è piuttosto sicuro che fosse noto presso gli antichi babilonesi, grazie al ritrovamento di un'iscrizione che accerta la conoscenza della relazione pitagorica. Il reperto, infatti, riporta il numero $\sqrt{2}$ corretto fino alle prime 6 cifre decimali, a testimonianza del fatto che il teorema di Pitagora doveva essere noto almeno in casi particolari.

È solo l'uomo greco, però, che ha voluto sapere perché vale. Si ha documentazione certa della sua dimostrazione con la proposizione 47 del libro I degli *Elementi* di Euclide. Anzi, tutte le precedenti 46 proposizioni sembrano date proprio per sostenere le ragioni del grande teorema. La tradizione, però, attribuisce a Pitagora la scoperta della dimostrazione.

La proposizione I.47, dall'edizione degli *Elementi* di Euclide di Cristoforo Clavio (1574).



Pitagora avrebbe conosciuto il metodo usato dai geometri egiziani per costruire l'angolo retto: prendevano una fune divisa in 12 parti uguali mediante nodi, come una collana; fissata la fune a terra con dei pioli a formare il triangolo di lati 3, 4 e 5 si ottiene un triangolo rettangolo. Perciò i geometri egiziani erano chiamati dai greci *arpedonapti*, ossia "annodatori" o "tenditori di funi".

Tavoletta d'argilla del periodo paleobabilonese della dinastia Hammurabi (XIX-XVII secolo a.C.) sulla quale è disegnato un quadrato di lato 30. Sulla diagonale sono riportati, scritti nei caratteri della numerazione sessagesimale in uso, i numeri 1,414213 (pari a $\sqrt{2}$) e 42,42639 ($30\sqrt{2}$).