Matematica: da strumento di tortura a regina delle scienze

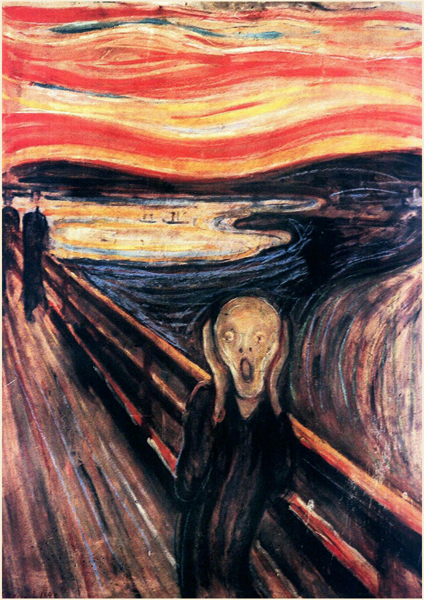
Alessandro Musesti

Università Cattolica del Sacro Cuore

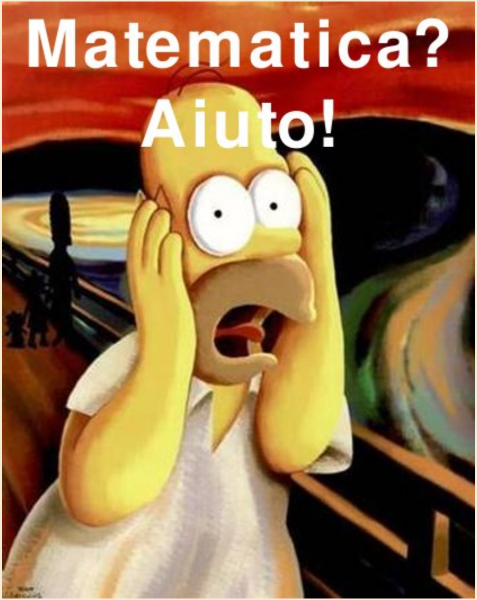
Desenzano del Garda, 30 ottobre 2009

Matematica come tortura

Matematica come tortura



Matematica come tortura



Matematica come tortura

Matematica come tortura

Matematica come tortura

FESTIVAL DELLA
MATEMATICA
LA REGINA DELLE
SCIENZE E DELLE ARTI

Matematica come tortura

FESTIVALDELLA
MATEMATICA2009
CREAZIONI E
RICREAZIONI

Esempi dai libri

(1.2) Definizione *Per ogni $m \geq 1$ e per ogni sottoinsieme E di $\mathbb{R}^n$ poniamo*

$$\mathcal{H}^m(E) := \alpha_m \sup_{\delta>0} \left(\inf \left\{ \sum_{h=0}^{\infty} (\operatorname{diam}(E_h))^m : \ E = \bigcup_{h=0}^{\infty} E_h, \ \operatorname{diam}(E_h) < \delta \right\} \right) ,$$

dove

$$\alpha_m := \left(\sup_{\delta>0} \left(\inf \left\{ \sum_{h=0}^{\infty} (\operatorname{diam}(E_h))^m : \ [0,1]^m = \bigcup_{h=0}^{\infty} E_h, \ \operatorname{diam}(E_h) < \delta \right\} \right) \right)^{-1} .$$

La funzione $\mathcal{H}^m : \mathfrak{P}(\mathbb{R}^n) \to [0, +\infty]$ si chiama misura esterna di Hausdorff $m-$dimensionale.

Esempi dai libri

L'angoloide.

1. Date in un certo ordine n ($n > 2$) **semirette** (fig. 1)

aventi l'origine in comune,

a tre a tre non complanari,

e tali che il piano individuato da due successive di esse lasci tutte le altre da una stessa parte,

dicesi angoloide *convesso* **(o, semplicemente, angoloide) l'intersezione degli** n **semispazi che hanno per origine quei piani e che contengono tutte le semirette date.**

Esempi dai libri

Infine, poichè date due classi contigue esiste una grandezza, ed una sola, minore di tutti gli elementi di una classe e maggiore di tutti quelli dell'altra, si può concludere, per il postulato precedentemente ammesso, col seguente

TEOREMA. **L'estensione della superficie laterale di un cilindro è l'elemento separatore delle due classi contigue delle estensioni delle superficie laterali dei prismi regolari inscritti e circoscritti al cilindro.**

Esempi dai libri

11. Trovare la diagonale di un rettangolo avente il perimetro di cm. 24 e nel quale il triplo del lato minore diminuito del lato maggiore è uguale alla differenza fra il lato maggiore e il minore. [*Risp. cm.* $4\sqrt{5}$]

Esempi dai libri

19. Due lati opposti di un parallelogramma sono il triplo degli altri due ed il perimetro è m. 120. La proiezione di un lato minore sul lato adiacente è la metà del lato stesso. Determinare il perimetro del triangolo equilatero equivalente al parallelogramma.

[*Risp. m.* $45\sqrt{6}$]

Esempi dai libri

Proprietà dell'addizione.

2. I. Proprietà commutativa. La somma di più numeri non cambia, mutando l'ordine degli addendi.

Esempio:

$$2 + 4 + 7 + 8 = 2 + 8 + 7 + 4.$$

II. Proprietà associativa. La somma di più numeri non cambia se a due o più di essi si sostituisce la loro somma.

Esempio:

$$2 + 9 + 11 + 5 = 2 + 20 + 5.$$

III. Proprietà dissociativa. La somma di due o più addendi non cambia se a uno di essi si sostituiscono più numeri la cui somma sia uguale all'addendo sostituito.

Esempio:

$$15 + 3 + 10 = 8 + 7 + 3 + 10.$$

Esempi dai libri

Proprietà dell'addizione.

2. I. Proprietà commutativa. La somma di più numeri non cambia, mutando l'ordine degli addendi.

Esempio:

$$2 + 4 + 7 + 8 = 2 + 8 + 7 + 4.$$

II. Proprietà associativa. La somma di più numeri non cambia se a due o più di essi si sostituisce la loro somma.

Esempio:

$$2 + 9 + 11 + 5 = 2 + 20 + 5.$$

III. Proprietà dissociativa. La somma di due o più addendi non cambia se a uno di essi si sostituiscono più numeri la cui somma sia uguale all'addendo sostituito.

Esempio:

$$15 + 3 + 10 = 8 + 7 + 3 + 10.$$

Esempi dai libri

La matematica è innanzitutto un *linguaggio*!

La Matematica deve la sua prima difficoltà al fatto che è *codificata*...

La matematica è innanzitutto un *linguaggio*!

La Matematica deve la sua prima difficoltà al fatto che è *codificata*...
Però, guardate questo esempio:

La matematica è innanzitutto un *linguaggio*!

La Matematica deve la sua prima difficoltà al fatto che è *codificata*...
Però, guardate questo esempio:

x dom tt ok

La matematica è innanzitutto un *linguaggio*!

La Matematica deve la sua prima difficoltà al fatto che è *codificata*...
Però, guardate questo esempio:

x dom tt ok

Ci avete capito qualcosa?

La matematica è innanzitutto un *linguaggio*!

La Matematica deve la sua prima difficoltà al fatto che è *codificata*...
Però, guardate questo esempio:

x dom tt ok

Ci avete capito qualcosa?
Se siete abbastanza giovani sì...

La matematica è innanzitutto un *linguaggio*!

La Matematica deve la sua prima difficoltà al fatto che è *codificata*...
Però, guardate questo esempio:

x dom tt ok

Ci avete capito qualcosa?
Se siete abbastanza giovani sì...

Per domani tutto a posto

La matematica è innanzitutto un *linguaggio*!

La Matematica deve la sua prima difficoltà al fatto che è *codificata*...
Però, guardate questo esempio:

x dom tt ok

Ci avete capito qualcosa?
Se siete abbastanza giovani sì...

Per domani tutto a posto

... è una parte di un sms!

Chi ha saputo leggere l'sms sarà stato facilitato dal fatto di conoscere l'italiano...

Chi ha saputo leggere l'sms sarà stato facilitato dal fatto di conoscere l'italiano...
Leggete ora questo:

Chi ha saputo leggere l'sms sarà stato facilitato dal fatto di conoscere l'italiano...
Leggete ora questo:

ВС ОК ДЛ ЗВ

Chi ha saputo leggere l'sms sarà stato facilitato dal fatto di conoscere l'italiano...
Leggete ora questo:

ВС ОК ДЛ ЗВ

Ci avete capito qualcosa?

Chi ha saputo leggere l'sms sarà stato facilitato dal fatto di conoscere l'italiano...
Leggete ora questo:

ВС ОК ДЛ ЗВ

Ci avete capito qualcosa?
Difficilmente...

È l'abbreviazione di un sms in cirillico...

È l'abbreviazione di un sms in cirillico...
che significa

È l'abbreviazione di un sms in cirillico...
che significa

все о'кеы для завтра

È l'abbreviazione di un sms in cirillico...
che significa

все о'кеы для завтра

e ancora è poco chiaro...

È l'abbreviazione di un sms in cirillico...
che significa

$$\text{все о'кеы для завтра}$$

e ancora è poco chiaro... significa "tutto ok per domani".

È l'abbreviazione di un sms in cirillico...
che significa

все о'кеы для завтра

e ancora è poco chiaro... significa "tutto ok per domani".
(beh, forse l'"ok" si era capito...)

È l'abbreviazione di un sms in cirillico...
che significa

$$\text{все о'кеы для завтра}$$

e ancora è poco chiaro... significa "tutto ok per domani".
(beh, forse l'"ok" si era capito...)
Queste sono le difficoltà della Matematica:

È l'abbreviazione di un sms in cirillico...
che significa

все о'кеы для завтра

e ancora è poco chiaro... significa "tutto ok per domani".
(beh, forse l'"ok" si era capito...)
Queste sono le difficoltà della Matematica:

1. Decifrare le abbreviazioni

È l'abbreviazione di un sms in cirillico...
che significa

все о'кеы для завтра

e ancora è poco chiaro... significa "tutto ok per domani".
(beh, forse l'"ok" si era capito...)
Queste sono le difficoltà della Matematica:

1. Decifrare le abbreviazioni
2. Leggere il messaggio

È l'abbreviazione di un sms in cirillico...
che significa

все о'кеы для завтра

e ancora è poco chiaro... significa "tutto ok per domani".
(beh, forse l'"ok" si era capito...)
Queste sono le difficoltà della Matematica:

1. Decifrare le abbreviazioni
2. Leggere il messaggio
3. Capire il messaggio

È l'abbreviazione di un sms in cirillico...
che significa

все о'кеы для завтра

e ancora è poco chiaro... significa "tutto ok per domani".
(beh, forse l'"ok" si era capito...)
Queste sono le difficoltà della Matematica:

1. Decifrare le abbreviazioni
2. Leggere il messaggio
3. Capire il messaggio

Guardate questo esempio:

$$\sqrt{x^2+2x+1} = |x+1|$$
$$x^2+2x+1 = 3x$$

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Prima difficoltà:

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Prima difficoltà: cos'è x? Cos'è x^2?

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Prima difficoltà: cos'è x? Cos'è x^2?
x è l'abbreviazione di un numero, che non viene scritto perché si può scegliere quello che si vuole (così la formula ha più valore); x^2 significa "x moltiplicato per x".

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Prima difficoltà: cos'è x? Cos'è x^2?
x è l'abbreviazione di un numero, che non viene scritto perché si può scegliere quello che si vuole (così la formula ha più valore); x^2 significa "x moltiplicato per x".
Seconda difficoltà:

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Prima difficoltà: cos'è x? Cos'è x^2?
x è l'abbreviazione di un numero, che non viene scritto perché si può scegliere quello che si vuole (così la formula ha più valore); x^2 significa "x moltiplicato per x".
Seconda difficoltà: cos'è quel $\sqrt{\ }$?

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Prima difficoltà: cos'è x? Cos'è x^2?
x è l'abbreviazione di un numero, che non viene scritto perché si può scegliere quello che si vuole (così la formula ha più valore); x^2 significa "x moltiplicato per x".
Seconda difficoltà: cos'è quel $\sqrt{\ }$?
$\sqrt{\ }$ sta a significare "la radice quadrata", ossia il numero che moltiplicato per se stesso dà il numero scritto sotto;

$$\sqrt{x^2+2x+1} = |x+1|$$
$$x^2+2x+1 = 3x$$

Prima difficoltà: cos'è x? Cos'è x^2?
x è l'abbreviazione di un numero, che non viene scritto perché si può scegliere quello che si vuole (così la formula ha più valore); x^2 significa "x moltiplicato per x".
Seconda difficoltà: cos'è quel $\sqrt{\ }$?
$\sqrt{\ }$ sta a significare "la radice quadrata", ossia il numero che moltiplicato per se stesso dà il numero scritto sotto;
Terza difficoltà:

$$\sqrt{x^2+2x+1} = |x+1|$$
$$x^2+2x+1 = 3x$$

Prima difficoltà: cos'è x? Cos'è x^2?
x è l'abbreviazione di un numero, che non viene scritto perché si può scegliere quello che si vuole (così la formula ha più valore); x^2 significa "x moltiplicato per x".
Seconda difficoltà: cos'è quel $\sqrt{\ }$?
$\sqrt{\ }$ sta a significare "la radice quadrata", ossia il numero che moltiplicato per se stesso dà il numero scritto sotto;
Terza difficoltà: cosa sono quelle barre scritte attorno all'$x+1$?

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Prima difficoltà: cos'è x? Cos'è x^2?
x è l'abbreviazione di un numero, che non viene scritto perché si può scegliere quello che si vuole (così la formula ha più valore); x^2 significa "x moltiplicato per x".
Seconda difficoltà: cos'è quel $\sqrt{\ }$?
$\sqrt{\ }$ sta a significare "la radice quadrata", ossia il numero che moltiplicato per se stesso dà il numero scritto sotto;
Terza difficoltà: cosa sono quelle barre scritte attorno all'$x + 1$?
Stanno a significare il "valore assoluto", cioè il "numero privato del segno" (come ahimé si dice);

e tt qst snz aver capito ancora nnt!

e tt qst snz aver capito ancora nnt!

(Trad.: e tutto questo senza aver capito ancora niente!)

e tt qst snz aver capito ancora nnt!

(Trad.: e tutto questo senza aver capito ancora niente!)

Questo infatti è il primo passo: *decodificare*.

e tt qst snz aver capito ancora nnt!

(Trad.: e tutto questo senza aver capito ancora niente!)

Questo infatti è il primo passo: *decodificare*.

Adesso viene la *lettura*:

e tt qst snz aver capito ancora nnt!

(Trad.: e tutto questo senza aver capito ancora niente!)

Questo infatti è il primo passo: *decodificare*.

Adesso viene la *lettura*:

> *"La radice quadrata di x al quadrato più due x più uno è uguale al valore assoluto di x più uno"*

e tt qst snz aver capito ancora nnt!

(Trad.: e tutto questo senza aver capito ancora niente!)

Questo infatti è il primo passo: *decodificare*.

Adesso viene la *lettura*:

> *"La radice quadrata di x al quadrato più due x più uno è uguale al valore assoluto di x più uno"*

e

e tt qst snz aver capito ancora nnt!

(Trad.: e tutto questo senza aver capito ancora niente!)

Questo infatti è il primo passo: *decodificare*.

Adesso viene la *lettura*:

> *"La radice quadrata di x al quadrato più due x più uno è uguale al valore assoluto di x più uno"*

e

> *"x al quadrato più due x più uno è uguale a tre x"*

e tt qst snz aver capito ancora nnt!

(Trad.: e tutto questo senza aver capito ancora niente!)

Questo infatti è il primo passo: *decodificare*.

Adesso viene la *lettura*:

> *"La radice quadrata di x al quadrato più due x più uno è uguale al valore assoluto di x più uno"*

e

> *"x al quadrato più due x più uno è uguale a tre x"*

Ma la parte più difficile deve ancora venire: la *comprensione*.

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$

$$x^2 + 2x + 1 = 3x$$

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Chi ha un po' di dimestichezza con la Matematica avrà subito notato che

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Chi ha un po' di dimestichezza con la Matematica avrà subito notato che

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$

$$\sqrt{x^2+2x+1} = |x+1|$$
$$x^2+2x+1 = 3x$$

Chi ha un po' di dimestichezza con la Matematica avrà subito notato che

$$\sqrt{x^2+2x+1} = |x+1|$$

e

$$\sqrt{x^2+2x+1} = |x+1|$$
$$x^2+2x+1 = 3x$$

Chi ha un po' di dimestichezza con la Matematica avrà subito notato che

$$\sqrt{x^2+2x+1} = |x+1|$$

e

$$x^2+2x+1 = 3x$$

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Chi ha un po' di dimestichezza con la Matematica avrà subito notato che

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$

e

$$x^2 + 2x + 1 = 3x$$

hanno due *significati* diversi:

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Chi ha un po' di dimestichezza con la Matematica avrà subito notato che

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$

e

$$x^2 + 2x + 1 = 3x$$

hanno due *significati* diversi:
la prima è un'*identità*, cioè vera sempre, o, come si dice, per ogni x;

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Chi ha un po' di dimestichezza con la Matematica avrà subito notato che

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$

e

$$x^2 + 2x + 1 = 3x$$

hanno due *significati* diversi:
la prima è un'*identità*, cioè vera sempre, o, come si dice, per ogni x;
la seconda è un'*equazione*, ossia un problema nel quale si cerca x in modo che la formula sia vera.

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$
$$x^2 + 2x + 1 = 3x$$

Chi ha un po' di dimestichezza con la Matematica avrà subito notato che

$$\sqrt{x^2 + 2x + 1} = |x + 1|$$

e

$$x^2 + 2x + 1 = 3x$$

hanno due *significati* diversi:
la prima è un'*identità*, cioè vera sempre, o, come si dice, per ogni x;
la seconda è un'*equazione*, ossia un problema nel quale si cerca x in modo che la formula sia vera.
Senza questa informazione sul significato, il senso della formula non si capisce.

La matematica "utile"

La matematica “utile”

- fotografia digitale: filtri, contorni, jpeg. . .

La matematica "utile"

- fotografia digitale: filtri, contorni, jpeg. . .

La matematica “utile”

- fotografia digitale: filtri, contorni, jpeg. . .

Trasformata discreta del coseno:

$$X_k = \frac{1}{2}(x_0 + (-1)^k x_{N-1}) + \sum_{n=1}^{N-2} x_n \cos\left[\frac{\pi}{N-1} nk\right] \qquad k = 0, \ldots, N-1.$$

La matematica “utile”

- fotografia digitale: filtri, contorni, jpeg...

Trasformata discreta di Fourier:

$$X_k = \sum_{n=0}^{N-1} x_n e^{-\frac{2\pi i}{N} kn} \qquad k = 0, \ldots, N-1$$

La matematica “utile”

- musica digitale: CD, mp3. . .

La matematica "utile"

- musica digitale: CD, mp3...

Fenomeno del mascheramento: l'orecchio umano non percepisce determinati suoni sovrapposti. In questo modo viene codificata minore informazione. Si usa di nuovo la trasformata del coseno e la trasformata di Fourier discreta.

La matematica “utile”

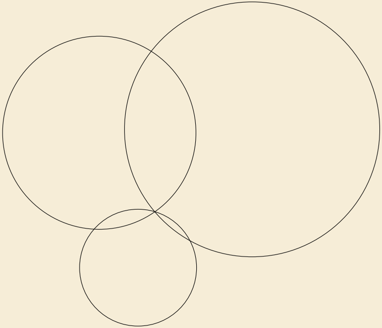
- film e tv digitali: alta definizione, dvd, satellite. . .

La matematica “utile”

- film e tv digitali: alta definizione, dvd, satellite. . .
- telefonia mobile, gps, navigatori satellitari

La matematica "utile"

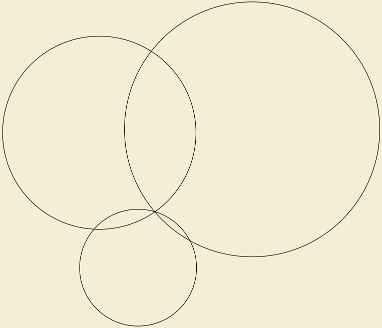
- film e tv digitali: alta definizione, dvd, satellite...
- telefonia mobile, gps, navigatori satellitari



L'intersezione di tre circonferenze individua un unico punto su una superficie.

La matematica “utile”

- film e tv digitali: alta definizione, dvd, satellite. . .
- telefonia mobile, gps, navigatori satellitari



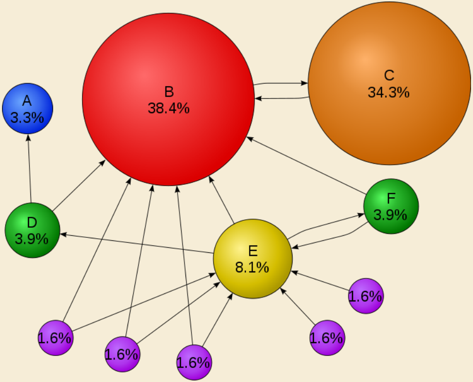
L’intersezione di tre circonferenze individua un unico punto su una superficie.
Bisogna considerare gli effetti relativistici!

La matematica "utile"

- internet (Google, ricerca di informazioni)

La matematica "utile"

- internet (Google, ricerca di informazioni)



L'algoritmo PageRank© di Google:

$$PR(p_i) = \frac{1-d}{N} + d \sum_{p_j \in M(p_i)} \frac{PR(p_j)}{L(p_j)}$$

La matematica “utile”

- La TAC (tomografia assiale computerizzata)
- la RMN (risonanza magnetica nucleare)

La matematica “utile”

- La TAC (tomografia assiale computerizzata)
- la RMN (risonanza magnetica nucleare)

TAC: trasformata di Radon

$$\mathcal{R}(m, q)[f(x, y)] = \int_{-\infty}^{\infty} f(x, mx + q)dx$$

La matematica “utile”

- La TAC (tomografia assiale computerizzata)
- la RMN (risonanza magnetica nucleare)

TAC: trasformata di Radon

$$\mathcal{R}(m,q)[f(x,y)] = \int_{-\infty}^{\infty} f(x, mx+q)dx$$

RMN: trasformata di Fourier

$$\mathcal{F}\{u\}(\boldsymbol{\omega}) = \frac{1}{\sqrt{2\pi}^n} \int_{\mathbb{R}^n} e^{-i\boldsymbol{\omega}\cdot\mathbf{t}} u(\mathbf{t})\, d\mathbf{t} \qquad \forall \boldsymbol{\omega} \in \mathbb{R}^n$$

La matematica "utile"

- previsioni del tempo

La matematica “utile”

- previsioni del tempo
- indagini statistiche, exit poll

La matematica "utile"

- previsioni del tempo
- indagini statistiche, exit poll
- analisi di rischio (assicurazioni)

La matematica “utile”

- previsioni del tempo
- indagini statistiche, exit poll
- analisi di rischio (assicurazioni)
- modelli finanziari

La matematica “utile”

- previsioni del tempo
- indagini statistiche, exit poll
- analisi di rischio (assicurazioni)
- modelli finanziari
- crittografia (bancomat, internet)

Matematica e sport

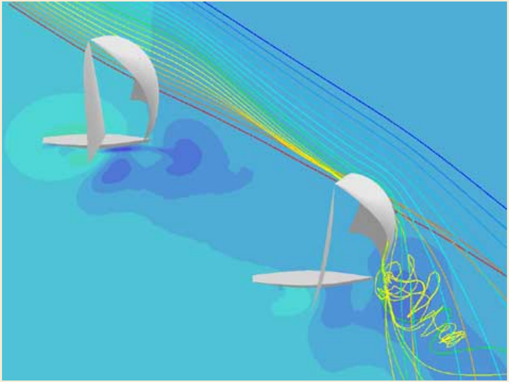
Uno dei successi più recenti delle "applicazioni" della matematica allo sport:

Matematica e sport

Uno dei successi più recenti delle "applicazioni" della matematica allo sport:

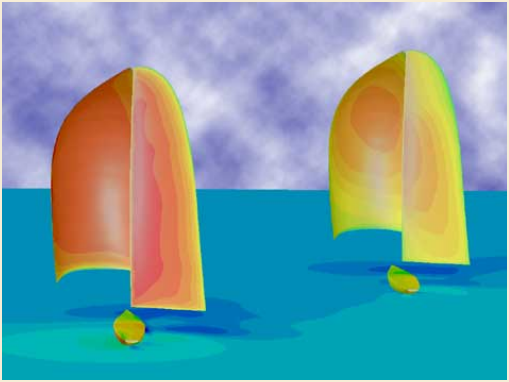
Matematica e sport

Uno dei successi più recenti delle "applicazioni" della matematica allo sport:



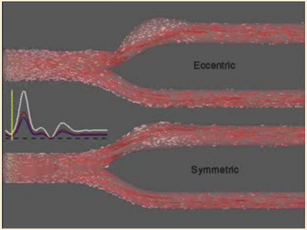
Matematica e sport

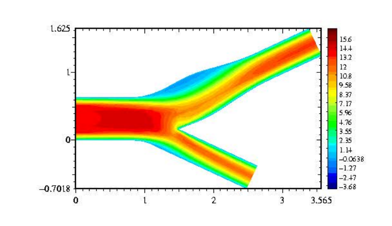
Uno dei successi più recenti delle "applicazioni" della matematica allo sport:



Matematica e medicina

Modelli e simulazioni mediche:





Matematica e finanza

Matematica e finanza

Matematica e finanza

Matematica e finanza

Questi economisti sono Fischer Black, Myron Scholes e Robert Merton. Gli ultimi due hanno preso il premio Nobel per l'economia nel 1997 (Black morì nel 1995).

Matematica e finanza

I loro studi sono spiccatamente matematici: la famosa formula di Black e Scholes si scrive così:

Matematica e finanza

I loro studi sono spiccatamente matematici: la famosa formula di Black e Scholes si scrive così:

$$
\begin{aligned}
C(S,t) &= SN(d_1) - Ke^{-r(T-t)}N(d_2) \\
d_1 &= \frac{\ln(S/K) + (r + \sigma^2/2)(T-t)}{\sigma\sqrt{T-t}} \\
d_2 &= d_1 - \sigma\sqrt{T-t}
\end{aligned}
$$

dove

$$
N(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp(-\xi^2/2)\, d\xi.
$$

Matematica e finanza

I loro studi sono spiccatamente matematici: la famosa formula di Black e Scholes si scrive così:

$$C(S,t) = SN(d_1) - Ke^{-r(T-t)}N(d_2)$$
$$d_1 = \frac{\ln(S/K) + (r + \sigma^2/2)(T-t)}{\sigma\sqrt{T-t}}$$
$$d_2 = d_1 - \sigma\sqrt{T-t}$$

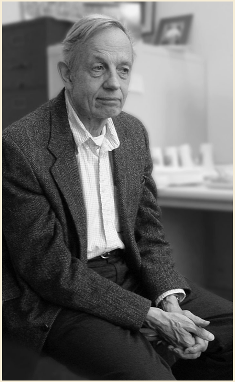
dove

$$N(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp(-\xi^2/2)\, d\xi.$$

(beh, prendiamola così...)

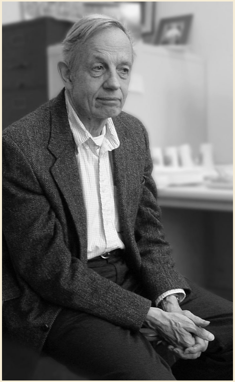
Matematica e finanza

Un altro matematico Nobel per l'economia è John Nash



Matematica e finanza

Un altro matematico Nobel per l'economia è John Nash



I suoi studi si concentrano sull'applicazione della *teoria dei giochi* alla finanza matematica.

Ed ecco infine un altro Nobel economico-matematico

Robert Aumann

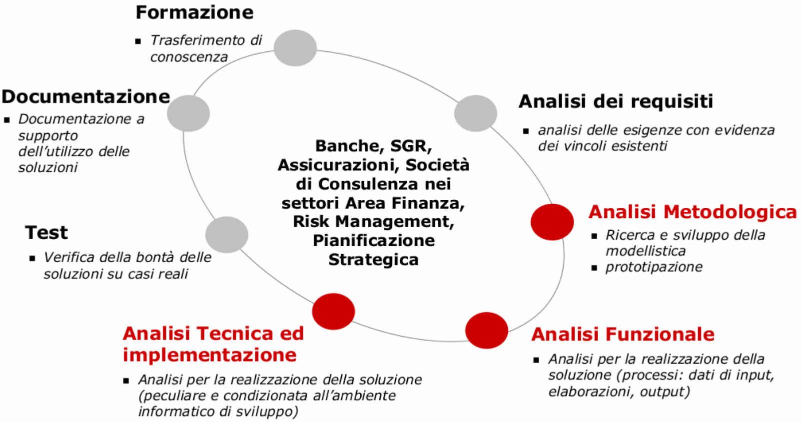
Ed ecco infine un altro Nobel economico-matematico

Robert Aumann

Anche lui ha introdotto le idee della teoria dei giochi nell'Economia.

Matematica e finanza

Il matematico trova la sua miglior collocazione nelle fasi di sviluppo metodologico, funzionale e tecnico-implementativo.



pagina: 8 Matematica e Finanza – Camilla Casciati

Matematica e finanza

La formula di Li

Matematica e finanza

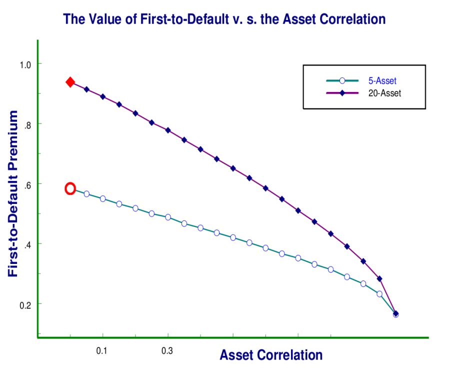
La formula di Li

$$\Pr[T_A < 1, T_B < 1] = \Phi_2(\Phi^{-1}(F_A(1)), \Phi^{-1}(F_B(1), \gamma)$$

Matematica e finanza

La formula di Li

$$\Pr[T_A < 1, T_B < 1] = \Phi_2(\Phi^{-1}(F_A(1)), \Phi^{-1}(F_B(1), \gamma)$$



Il Superenalotto

Nel gioco del Superenalotto bisogna indovinare 6 numeri estratti tra i primi 90.

Il Superenalotto

Nel gioco del Superenalotto bisogna indovinare 6 numeri estratti tra i primi 90.
Per calcolare quante combinazioni diverse ci sono, pensiamo che il primo numero estratto ha 90 possibilità diverse,

Il Superenalotto

Nel gioco del Superenalotto bisogna indovinare 6 numeri estratti tra i primi 90.
Per calcolare quante combinazioni diverse ci sono, pensiamo che il primo numero estratto ha 90 possibilità diverse, il secondo ne ha 89 (visto che già ne manca uno dall'urna),

Il Superenalotto

Nel gioco del Superenalotto bisogna indovinare 6 numeri estratti tra i primi 90.
Per calcolare quante combinazioni diverse ci sono, pensiamo che il primo numero estratto ha 90 possibilità diverse, il secondo ne ha 89 (visto che già ne manca uno dall'urna), il terzo 88,

Il Superenalotto

Nel gioco del Superenalotto bisogna indovinare 6 numeri estratti tra i primi 90.
Per calcolare quante combinazioni diverse ci sono, pensiamo che il primo numero estratto ha 90 possibilità diverse, il secondo ne ha 89 (visto che già ne manca uno dall'urna), il terzo 88, il quarto 87, il quinto 86, il sesto 85.

Il Superenalotto

Nel gioco del Superenalotto bisogna indovinare 6 numeri estratti tra i primi 90.
Per calcolare quante combinazioni diverse ci sono, pensiamo che il primo numero estratto ha 90 possibilità diverse, il secondo ne ha 89 (visto che già ne manca uno dall'urna), il terzo 88, il quarto 87, il quinto 86, il sesto 85.
In totale si hanno

$$90 \cdot 89 \cdot 88 \cdot 87 \cdot 86 \cdot 85 = 448\,282\,533\,600$$

possibilità diverse.

Il Superenalotto

Nel gioco del Superenalotto bisogna indovinare 6 numeri estratti tra i primi 90.
Per calcolare quante combinazioni diverse ci sono, pensiamo che il primo numero estratto ha 90 possibilità diverse, il secondo ne ha 89 (visto che già ne manca uno dall'urna), il terzo 88, il quarto 87, il quinto 86, il sesto 85.
In totale si hanno

$$90 \cdot 89 \cdot 88 \cdot 87 \cdot 86 \cdot 85 = 448\,282\,533\,600$$

possibilità diverse.
Per fortuna, però, i numeri non vanno indovinati nell'ordine di estrazione:

Il Superenalotto

Nel gioco del Superenalotto bisogna indovinare 6 numeri estratti tra i primi 90.
Per calcolare quante combinazioni diverse ci sono, pensiamo che il primo numero estratto ha 90 possibilità diverse, il secondo ne ha 89 (visto che già ne manca uno dall'urna), il terzo 88, il quarto 87, il quinto 86, il sesto 85.
In totale si hanno

$$90 \cdot 89 \cdot 88 \cdot 87 \cdot 86 \cdot 85 = 448\,282\,533\,600$$

possibilità diverse.
Per fortuna, però, i numeri non vanno indovinati nell'ordine di estrazione: poiché i modi di riordinare 6 numeri sono $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 720$, le possibili colonne vincenti del Superenalotto si riducono a

$$448\,282\,533\,600/720 = 622\,614\,630$$

ovvero oltre 622 milioni.

Il Superenalotto

Nel gioco del Superenalotto bisogna indovinare 6 numeri estratti tra i primi 90.
Per calcolare quante combinazioni diverse ci sono, pensiamo che il primo numero estratto ha 90 possibilità diverse, il secondo ne ha 89 (visto che già ne manca uno dall'urna), il terzo 88, il quarto 87, il quinto 86, il sesto 85.
In totale si hanno

$$90 \cdot 89 \cdot 88 \cdot 87 \cdot 86 \cdot 85 = 448\,282\,533\,600$$

possibilità diverse.
Per fortuna, però, i numeri non vanno indovinati nell'ordine di estrazione: poiché i modi di riordinare 6 numeri sono $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 720$, le possibili colonne vincenti del Superenalotto si riducono a

$$448\,282\,533\,600/720 = 622\,614\,630$$

ovvero oltre 622 milioni. Vuol dire che abbiamo una probabilità su oltre 622 milioni di indovinare la colonna vincente.

Il Superenalotto

Considerato che ogni colonna costa 50 centesimi di euro, una vincita "equa" per questo gioco sarebbe di circa 311 milioni di euro.

Il Superenalotto

Considerato che ogni colonna costa 50 centesimi di euro, una vincita “equa” per questo gioco sarebbe di circa 311 milioni di euro.
La vincita più alta (22 agosto di quest’anno) ha pagato 148 milioni.

Il Superenalotto

Considerato che ogni colonna costa 50 centesimi di euro, una vincita "equa" per questo gioco sarebbe di circa 311 milioni di euro.
La vincita più alta (22 agosto di quest'anno) ha pagato 148 milioni.

Il Superenalotto non è per niente equo!

Il Superenalotto

Considerato che ogni colonna costa 50 centesimi di euro, una vincita "equa" per questo gioco sarebbe di circa 311 milioni di euro.
La vincita più alta (22 agosto di quest'anno) ha pagato 148 milioni.

Il Superenalotto non è per niente equo!

Come se non bastasse, si è aggiunto anche il numero "SuperStar", ovvero un settimo numero indipendente da tutti gli altri.

Considerato che ogni colonna costa 50 centesimi di euro, una vincita "equa" per questo gioco sarebbe di circa 311 milioni di euro.
La vincita più alta (22 agosto di quest'anno) ha pagato 148 milioni.

Il Superenalotto non è per niente equo!

Come se non bastasse, si è aggiunto anche il numero "SuperStar", ovvero un settimo numero indipendente da tutti gli altri.
La probabilità di indovinare tutti e sei i numeri più il numero Superstar viene ulteriormente divisa per 90, dando una probabilità su oltre 56 miliardi (per la precisione una probabilità su 56 035 316 700).

Considerato che ogni colonna costa 50 centesimi di euro, una vincita "equa" per questo gioco sarebbe di circa 311 milioni di euro.
La vincita più alta (22 agosto di quest'anno) ha pagato 148 milioni.

Il Superenalotto non è per niente equo!

Come se non bastasse, si è aggiunto anche il numero "SuperStar", ovvero un settimo numero indipendente da tutti gli altri.
La probabilità di indovinare tutti e sei i numeri più il numero Superstar viene ulteriormente divisa per 90, dando una probabilità su oltre 56 miliardi (per la precisione una probabilità su 56 035 316 700).
Quindi la matematica ci insegna a

Il Superenalotto

Considerato che ogni colonna costa 50 centesimi di euro, una vincita "equa" per questo gioco sarebbe di circa 311 milioni di euro.
La vincita più alta (22 agosto di quest'anno) ha pagato 148 milioni.

Il Superenalotto non è per niente equo!

Come se non bastasse, si è aggiunto anche il numero "SuperStar", ovvero un settimo numero indipendente da tutti gli altri.
La probabilità di indovinare tutti e sei i numeri più il numero Superstar viene ulteriormente divisa per 90, dando una probabilità su oltre 56 miliardi (per la precisione una probabilità su 56 035 316 700).
Quindi la matematica ci insegna a

non giocare al Superenalotto!

Matematica e crittografia

Numeri primi: sono i numeri divisibili solo per se stessi (e per 1, ovviamente).

Matematica e crittografia

Numeri primi: sono i numeri divisibili solo per se stessi (e per 1, ovviamente).
Sono infiniti: 2, 3, 5, 7, 11, 13, 17, ..., $2^{43.112.609} - 1$, ...

Matematica e crittografia

Numeri primi: sono i numeri divisibili solo per se stessi (e per 1, ovviamente).
Sono infiniti: 2, 3, 5, 7, 11, 13, 17, $\ldots$, $2^{43.112.609} - 1$, $\ldots$
(I'ultimo numero scritto ha quasi 13 milioni di cifre!)

Matematica e crittografia

Numeri primi: sono i numeri divisibili solo per se stessi (e per 1, ovviamente).

Sono infiniti: $2, 3, 5, 7, 11, 13, 17, \ldots, 2^{43.112.609} - 1, \ldots$

(l'ultimo numero scritto ha quasi 13 milioni di cifre!)

Ma servono a qualcosa???

Matematica e crittografia

Numeri primi: sono i numeri divisibili solo per se stessi (e per 1, ovviamente).
Sono infiniti: $2, 3, 5, 7, 11, 13, 17, \dots, 2^{43.112.609} - 1, \dots$
(l'ultimo numero scritto ha quasi 13 milioni di cifre!)

Ma servono a qualcosa???

L'algoritmo RSA (Ronald Rivest, Adi Shamir e Leonard Adleman) è usato in quasi tutte le transazioni economiche online

Numeri primi: sono i numeri divisibili solo per se stessi (e per 1, ovviamente).
Sono infiniti: $2, 3, 5, 7, 11, 13, 17, \ldots, 2^{43.112.609} - 1, \ldots$
(I'ultimo numero scritto ha quasi 13 milioni di cifre!)

Ma servono a qualcosa???

L'algoritmo RSA (Ronald Rivest, Adi Shamir e Leonard Adleman) è usato in quasi tutte le transazioni economiche online

e si basa sui numeri primi!

Matematica e crittografia

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

Matematica e crittografia

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

si prende un numero primo d più piccolo di $(p-1)(q-1)$

Matematica e crittografia

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

si prende un numero primo d più piccolo di $(p-1)(q-1)$

Si cerca un numero e per cui il resto di $e \cdot d$ diviso $(p-1)(q-1)$ faccia proprio 1.

Matematica e crittografia

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

si prende un numero primo d più piccolo di $(p-1)(q-1)$

Si cerca un numero e per cui il resto di $e \cdot d$ diviso $(p-1)(q-1)$ faccia proprio 1.

Ad esempio:

Matematica e crittografia

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

si prende un numero primo d più piccolo di $(p-1)(q-1)$

Si cerca un numero e per cui il resto di $e \cdot d$ diviso $(p-1)(q-1)$ faccia proprio 1.

Ad esempio: $p = 3$, $q = 19$, quindi

Matematica e crittografia

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

si prende un numero primo d più piccolo di $(p-1)(q-1)$

Si cerca un numero e per cui il resto di $e \cdot d$ diviso $(p-1)(q-1)$ faccia proprio 1.

Ad esempio: $p = 3$, $q = 19$, quindi $N = 57$ e $(p-1)(q-1) = 36$.

Matematica e crittografia

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

si prende un numero primo d più piccolo di $(p-1)(q-1)$

Si cerca un numero e per cui il resto di $e \cdot d$ diviso $(p-1)(q-1)$ faccia proprio 1.

Ad esempio: $p = 3$, $q = 19$, quindi $N = 57$ e $(p-1)(q-1) = 36$.
Scegliamo $d = 29$.

Matematica e crittografia

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

si prende un numero primo d più piccolo di $(p-1)(q-1)$

Si cerca un numero e per cui il resto di $e \cdot d$ diviso $(p-1)(q-1)$ faccia proprio 1.

Ad esempio: $p = 3$, $q = 19$, quindi $N = 57$ e $(p-1)(q-1) = 36$. Scegliamo $d = 29$.

Si verifica che per $e = 5$ si ha che il resto di $29 \cdot 5 : 36$ dà 1.

Matematica e crittografia

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

si prende un numero primo d più piccolo di $(p-1)(q-1)$

Si cerca un numero e per cui il resto di $e \cdot d$ diviso $(p-1)(q-1)$ faccia proprio 1.

Ad esempio: $p = 3$, $q = 19$, quindi $N = 57$ e $(p-1)(q-1) = 36$. Scegliamo $d = 29$.

Si verifica che per $e = 5$ si ha che il resto di $29 \cdot 5 : 36$ dà 1.

Ora: se solo noi conosciamo 29 e rendiamo pubblico $(57, 5)$, se qualcuno ci vuol comunicare il numero $m = 10$ fa così:

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

si prende un numero primo d più piccolo di $(p-1)(q-1)$

Si cerca un numero e per cui il resto di $e \cdot d$ diviso $(p-1)(q-1)$ faccia proprio 1.

Ad esempio: $p = 3$, $q = 19$, quindi $N = 57$ e $(p-1)(q-1) = 36$.
Scegliamo $d = 29$.

Si verifica che per $e = 5$ si ha che il resto di $29 \cdot 5 : 36$ dà 1.

Ora: se solo noi conosciamo 29 e rendiamo pubblico $(57, 5)$, se qualcuno ci vuol comunicare il numero $m = 10$ fa così:
prende $(57, 5)$ che è pubblica e calcola il resto di $10^5 : 57$

Matematica e crittografia

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

si prende un numero primo d più piccolo di $(p-1)(q-1)$

Si cerca un numero e per cui il resto di $e \cdot d$ diviso $(p-1)(q-1)$ faccia proprio 1.

Ad esempio: $p = 3$, $q = 19$, quindi $N = 57$ e $(p-1)(q-1) = 36$.
Scegliamo $d = 29$.

Si verifica che per $e = 5$ si ha che il resto di $29 \cdot 5 : 36$ dà 1.

Ora: se solo noi conosciamo 29 e rendiamo pubblico $(57, 5)$, se qualcuno ci vuol comunicare il numero $m = 10$ fa così:
prende $(57, 5)$ che è pubblica e calcola il resto di $10^5 : 57$ (viene 22)

Matematica e crittografia

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

si prende un numero primo d più piccolo di $(p-1)(q-1)$

Si cerca un numero e per cui il resto di $e \cdot d$ diviso $(p-1)(q-1)$ faccia proprio 1.

Ad esempio: $p = 3$, $q = 19$, quindi $N = 57$ e $(p-1)(q-1) = 36$.
Scegliamo $d = 29$.

Si verifica che per $e = 5$ si ha che il resto di $29 \cdot 5 : 36$ dà 1.

Ora: se solo noi conosciamo 29 e rendiamo pubblico $(57, 5)$, se qualcuno ci vuol comunicare il numero $m = 10$ fa così:
prende $(57, 5)$ che è pubblica e calcola il resto di $10^5 : 57$ (viene 22)
e ci comunica il risultato. Noi poi calcoliamo 22^{29} usando la nostra chiave privata, e ne prendiamo al solito il resto della divisione per 57:

Si prende N come prodotto di due numeri primi, $N = p \cdot q$

si prende un numero primo d più piccolo di $(p-1)(q-1)$

Si cerca un numero e per cui il resto di $e \cdot d$ diviso $(p-1)(q-1)$ faccia proprio 1.

Ad esempio: $p = 3$, $q = 19$, quindi $N = 57$ e $(p-1)(q-1) = 36$. Scegliamo $d = 29$.

Si verifica che per $e = 5$ si ha che il resto di $29 \cdot 5 : 36$ dà 1.

Ora: se solo noi conosciamo 29 e rendiamo pubblico $(57, 5)$, se qualcuno ci vuol comunicare il numero $m = 10$ fa così:
prende $(57, 5)$ che è pubblica e calcola il resto di $10^5 : 57$ (viene 22)
e ci comunica il risultato. Noi poi calcoliamo 22^{29} usando la nostra chiave privata, e ne prendiamo al solito il resto della divisione per 57:

risulta 10

Nella pratica, anche conoscendo $(57, 5)$ è difficile trovare il 29, che si chiama *chiave privata*.

Nella pratica, anche conoscendo $(57, 5)$ è difficile trovare il 29, che si chiama *chiave privata*.

Bisogna andare per tentativi.

Matematica e crittografia

Nella pratica, anche conoscendo $(57, 5)$ è difficile trovare il 29, che si chiama *chiave privata*.

Bisogna andare per tentativi.

Una tattica consiste nel fattorizzare N: nell'esempio, $N = 57 = 3 \cdot 19$,

Matematica e crittografia

Nella pratica, anche conoscendo $(57, 5)$ è difficile trovare il 29, che si chiama *chiave privata*.

Bisogna andare per tentativi.

Una tattica consiste nel fattorizzare N: nell'esempio, $N = 57 = 3 \cdot 19$,

quindi si può trovare $(p - 1)(q - 1) = 36$ da cui, noto il 5 che sta nella *chiave pubblica*, si può ricavare il 29 e quindi decifrare ogni messaggio.

Matematica e crittografia

Nella pratica, anche conoscendo $(57, 5)$ è difficile trovare il 29, che si chiama *chiave privata*.

Bisogna andare per tentativi.

Una tattica consiste nel fattorizzare N: nell'esempio, $N = 57 = 3 \cdot 19$,

quindi si può trovare $(p-1)(q-1) = 36$ da cui, noto il 5 che sta nella *chiave pubblica*, si può ricavare il 29 e quindi decifrare ogni messaggio. Ma se avessimo avuto

1751952685614616185916001760791655006749 ? (40 cifre!)

Matematica e crittografia

Nella pratica, anche conoscendo $(57, 5)$ è difficile trovare il 29, che si chiama *chiave privata*.

Bisogna andare per tentativi.

Una tattica consiste nel fattorizzare N: nell'esempio, $N = 57 = 3 \cdot 19$,

quindi si può trovare $(p-1)(q-1) = 36$ da cui, noto il 5 che sta nella *chiave pubblica*, si può ricavare il 29 e quindi decifrare ogni messaggio. Ma se avessimo avuto

$$1751952685614616185916001760791655006749 \text{ ?} \qquad \text{(40 cifre!)}$$
$$= 48112959837082048697 \cdot 36413321723440003717$$

Matematica e crittografia

Nella pratica, anche conoscendo $(57, 5)$ è difficile trovare il 29, che si chiama *chiave privata*.

Bisogna andare per tentativi.

Una tattica consiste nel fattorizzare N: nell'esempio, $N = 57 = 3 \cdot 19$,

quindi si può trovare $(p-1)(q-1) = 36$ da cui, noto il 5 che sta nella *chiave pubblica*, si può ricavare il 29 e quindi decifrare ogni messaggio. Ma se avessimo avuto

$$1751952685614616185916001760791655006749 \text{ ?} \qquad \text{(40 cifre!)}$$
$$= 48112959837082048697 \cdot 36413321723440003717$$

E nelle transazioni si usano di solito numeri primi di più di 300 cifre!

Matematica e crittografia

Nella pratica, anche conoscendo $(57, 5)$ è difficile trovare il 29, che si chiama *chiave privata*.

Bisogna andare per tentativi.

Una tattica consiste nel fattorizzare N: nell'esempio, $N = 57 = 3 \cdot 19$,

quindi si può trovare $(p-1)(q-1) = 36$ da cui, noto il 5 che sta nella *chiave pubblica*, si può ricavare il 29 e quindi decifrare ogni messaggio. Ma se avessimo avuto

$$\begin{aligned} &1751952685614616185916001760791655006749 \text{ ?} \qquad \text{(40 cifre!)} \\ &= 48112959837082048697 \cdot 36413321723440003717 \end{aligned}$$

E nelle transazioni si usano di solito numeri primi di più di 300 cifre! Sarebbero richieste centinaia di anni di calcoli con un super-computer. . .

Nella pratica, anche conoscendo $(57, 5)$ è difficile trovare il 29, che si chiama *chiave privata*.

Bisogna andare per tentativi.

Una tattica consiste nel fattorizzare N: nell'esempio, $N = 57 = 3 \cdot 19$,

quindi si può trovare $(p-1)(q-1) = 36$ da cui, noto il 5 che sta nella *chiave pubblica*, si può ricavare il 29 e quindi decifrare ogni messaggio. Ma se avessimo avuto

$$1751952685614616185916001760791655006749 \text{ ?} \qquad \text{(40 cifre!)}$$
$$= 48112959837082048697 \cdot 36413321723440003717$$

E nelle transazioni si usano di solito numeri primi di più di 300 cifre! Sarebbero richieste centinaia di anni di calcoli con un super-computer...

a meno di non trovare un metodo alternativo

Matematica e crittografia

Nella pratica, anche conoscendo $(57, 5)$ è difficile trovare il 29, che si chiama *chiave privata*.

Bisogna andare per tentativi.

Una tattica consiste nel fattorizzare N: nell'esempio, $N = 57 = 3 \cdot 19$,

quindi si può trovare $(p-1)(q-1) = 36$ da cui, noto il 5 che sta nella *chiave pubblica*, si può ricavare il 29 e quindi decifrare ogni messaggio. Ma se avessimo avuto

$$1751952685614616185916001760791655006749 \text{ ?} \qquad \text{(40 cifre!)}$$
$$= 48112959837082048697 \cdot 36413321723440003717$$

E nelle transazioni si usano di solito numeri primi di più di 300 cifre! Sarebbero richieste centinaia di anni di calcoli con un super-computer...

a meno di non trovare un metodo alternativo (che nessuno ha ancora scoperto!)

Una citazione famosa

[L'universo] è scritto in lingua matematica, e i caratteri son triangoli, cerchi, ed altre figure geometriche, senza i quali mezzi è impossibile a intenderne umanamente parola; senza questi è un aggirarsi vanamente per un oscuro laberinto.

Una citazione famosa

[L'universo] è scritto in lingua matematica, e i caratteri son triangoli, cerchi, ed altre figure geometriche, senza i quali mezi è impossibile a intenderne umanamente parola; senza questi è un aggirarsi vanamente per un oscuro laberinto.

Galileo Galilei, da "Il Saggiatore"