magazine
MATEMATICAMENTE.IT
Rivista trimestrale di matematica per curiosi e appassionati distribuita gratuitamente sul sito

• Numero 15 – Maggio 2011 •

I am a camera
by Daniel n. reid
http://www.flickr.com/photos/daniel_n_reid/5144410/

RENDIMENTI BCE – CONGETTURE DI ERDOS – CRITTOGRAFIA– MOLTIPLICAZIONE – FRAZIONI – RETICOLO DELLA DAMA – TEORIA DEI MODELLI- LIBRI

Come proporre un contributo
Istruzioni per gli autori

La rivista pubblica articoli, interviste, buone pratiche e giochi relativamente alla matematica e alle sue applicazioni.
Lo stile, la terminologia e le idee espresse devono essere chiari e accessibili a tutti.
Gli articoli saranno valutati da uno o più collaboratori esperti in materia. La Redazione si riserva, dopo ponderato esame, la decisione di pubblicare o non pubblicare il lavoro ricevuto.
In caso di accettata pubblicazione, sarà cura della Direzione informare gli autori dell'accettazione; l'articolo sarà pubblicato in forma elettronica così come è, salvo eventuali interventi redazionali, anche sul contenuto, per migliorarne la fruibilità da parte del lettore.
È possibile che la Redazione subordini la pubblicazione dell'articolo a modifiche anche sostanziali che devono essere fatte dall'autore. I contributi devono essere inviati in forma elettronica al direttore responsabile.
Gli articoli o gli altri tipi di contributi devono essere in formato .doc, .docx, .rtf, .odt o formati analoghi. Le formule possono essere in Microsoft Equation Editor, MathType, Open office math o immagini nei formati gif, jpeg, png, tif. Sono ammesse figure, tabelle e grafici purché estremamente curati e inviati in file a parte. Di ogni elemento non testuale deve essere indicata la posizione precisa all'interno del testo. Se le immagini utilizzate sono protette da diritti d'autore, sarà cura dell'autore dell'articolo ottenere le autorizzazioni necessarie.
Nella prima pagina andranno indicati: titolo del lavoro, nome e cognome degli autori, qualifica professionale e istituzione o ambiente professionale di appartenenza, indirizzo e-mail.
L'articolo dovrà iniziare con un breve sunto (5-10 righe) preferibilmente in italiano e in inglese, e dovrà terminare con una bibliografia.
I riferimenti bibliografici devono essere indicati all'interno del testo nel seguente modo: [3] oppure [Ba], se si deve indicare la pagina usare [Ba, p.15].
Le note al testo dovrebbero essere in generale evitate; sono preferiti all'interno del testo rimandi alla bibliografia.
I contributi non devono complessivamente superare le 12 pagine.

La Redazione non garantisce la correttezza scientifica del contenuto degli articoli. Gli autori sono responsabili del contenuto dei testi inviati per la pubblicazione.
Se l'articolo è stato pubblicato in altra sede l'autore deve richiederne l'autorizzazione a chi ha pubblicato per primo l'articolo e fornire le coordinate alla Redazione.

MATEMATICAMENTE.IT MAGAZINE
Rivista trimestrale di matematica per curiosi e appassionati distribuita gratuitamente sul sito www.matematicamente.it

Registrazione del 19.12.2006 al n.953 del Tribunale di Lecce
ISSN 2035-0449

Direttore responsabile
Antonio Bernardo
antoniobernardo@matematicamente.it

Vicedirettore
Luca Lussardi
lucalussardi@matematicamente.it

Redazione
Flavio Cimolin
flaviocimolin@matematicamente.it
Diego Alberto - Luca Barletta - Michele Mazzucato - Nicola Chiriano

Hanno collaborato a questo numero
Stefano Borgogni, Roberto Chiappi, Cosimo De Mitri, Domenico Lenzi, Pietro Romano, Marco Ruffinoni, Carlo Sintini, GabrieleTaddei, Riccardo Travaglini.

Sommario

Editoriale

In questo numero, Gabriella D'Agostino e Antonio Guglielmi ci parlano di tassi di mercato delle attività finanziarie, di politiche di gestione del rischio dei tassi di interesse… questioni di particolare attualità. Andreana Zucco ci presenta tre congetture di Erdös riguardanti insiemi composti da un numero finito di punti nel piano. Gianluca Salvalaggio ci descrive il fascino dei numeri primi e la loro più classica applicazione alla crittografia a chiave pubblica. Michele Mazzucato fa una scheda sintetica della moltiplicazione nella sua evoluzione storica, i metodi antichi e più moderni per moltiplicare due numeri interi. Domenico Lenzi e Ilario Marra fanno alcune riflessioni sull'insegnamento delle frazioni nella scuola dell'obbligo e presentano alcune metodologie innovative. Bruno Sanchini ci dà una possibile descrizione analitica del reticolo della dama. Paolo Bonicatto ci introduce alla Teoria dei modelli.

Antonio Bernardo

151. Il modello matematico sottostante alla curva dei rendimenti della BCE

di Gabriella D'Agostino[1], Antonio Guglielmi[2]
{gabriella.dagostino; antonio.guglielmi}@unisalento.it
[Dip. SEMS - Università del Salento]

Sunto

I tassi d'interesse sono grandezze finanziarie non direttamente quotate sui mercati finanziari, infatti sono ricavati da altri strumenti finanziari il cui prezzo, invece, viene registrato sui mercati.
Le informazioni implicite nei tassi di mercato di diverse attività finanziarie forniscono indicazioni prospettiche sulle aspettative del mercato riguardo a numerosi fattori fondamentali, come l'evoluzione futura delle attività economiche e l'inflazione, nonché l'andamento del costo del denaro. L'analisi di tali aspettative è importante per l'attuazione di politiche di gestione del rischio di tasso d'interesse [ADGS].
La curva dei rendimenti è la curva che si ottiene dalla relazione che lega l'evoluzione del rendimento di un titolo rispetto alla scadenza dello stesso.
Molti modelli sono stati proposti negli ultimi anni per stimare la curva dei rendimenti, alcuni basati direttamente sul prezzo di titoli a reddito certo (titoli a cedola nulla e titoli a cedola certa) e maturity (scadenza) in funzione di alcuni parametri (*cross-sectional dimension*), ad esempio il modello di Neson-Siegel (1987) [NS], il modello di estensione di Svensson (1994) [S] (o modello di Nelson-Siegel-Svensson), altri basati sulla specificazione esogena delle dinamiche di alcun rilevanti fattori (time-series dimension), come ad esempio il modello di Vasicek (1977) [V] ed il modello di Cox–Ingersoll-Ross (1985) [CIR].
Lo scopo principale di questo contributo è introdurre e discutere il modello utilizzato dalla banca Centrale Europea (BCE) per la stima della curva dei rendimenti, ovvero la cosiddetta struttura per scadenza dei rendimenti.
Verrà dapprima discusso il modello di valutazione di Nelson – Siegel – Svensson e successivamente verrà discussa l'applicazione che ne fa la BCE.

Classificazione AMS: 91B24; 62M20.
Classificazione JEL: G120.
Parole chiave: curva dei rendimenti, modello di Nelson – Siegel – Svensson, stima dei parametri, strutture per scadenza risk-free BCE.

Introduzione e principali definizioni

La funzione di sconto (o funzione valore) è quella relazione di equivalenza finanziaria intertemporale attraverso la quale è possibile determinare l'importo $P(t,T,s)$ che concordato al tempo t (stipula) deve essere versato in T (valuta) per ricevere alla scadenza del contratto s una posta unitaria. La differenza $(s-T)$ è la durata del contratto o maturity. Se la data di stipula coincide con la data di valuta $(t=T)$ il contratto si definisce a pronti e la funzione valore si indica con $P(t,s)$, mentre se $(t \neq T)$ il contratto si definisce a termine e la funzione valore è espressa da $P(t,T,s)$[3]. Pertanto il valore attualizzato, ovvero il valore al tempo t di un importo X_s disponibile al tempo s sarà

$$X_t = X_s \cdot P(t,s) \qquad (1)$$

[1] Dottore di Ricerca in "Scienze Matematico – Statistiche per la Finanza e la Geostatistica" – Indirizzo Finanza.
[2] Dottorando di Ricerca in "Scienze Economiche e Matematico – Statistiche" – Indirizzo Finanza.
[3] Per una trattazione analitica delle proprietà della funzione valore vedi [M].

Allo stesso tempo possiamo affermare che X_t è la quantità di denaro da versare al tempo t per avere una quantità di denaro X_s disponibile al tempo s.
Il valore $W(t,X)$ del vettore dei flussi X, dato da un titolo che paga cedole costanti dell'importo c e che rimborsa a scadenza il valore nominale C con maturity N, su un vettore di tempi $\{t_1,t_2,.....t_N\}$ al tempo t sarà

$$W(t,X)=c\cdot P(t,t_1)+c\cdot P(t,t_2)+.....+(c+C)\cdot P(t,t_N) \qquad (2)$$

La curva dei rendimenti a scadenza $R(t,s)$ è definita dalla seguente relazione

$$P(t,s)=\exp(-(s-t)\cdot R(t,s)) \quad \Leftrightarrow \quad R(t,s)=-\frac{1}{s-t}\ln P(t,s) \qquad (3)$$

Un'altra quantità importante è l'intensità istantanea d'interesse $f(t,s)$, che è definito dalla seguente relazione

$$P(t,s)=\exp\left(-\int_t^s f(t,u)du\right) \quad \Leftrightarrow \quad f(t,s)=-\frac{\partial}{\partial s}\ln P(t,s) \qquad (4)$$

Il tasso d'interesse $i(t,s)$ è dato dalla seguente relazione

$$i(t,s)=(P(t,s))^{t-s}-1 \qquad (5)$$

Pertanto, dato un insieme Ω di titoli obbligazionari, con diverse scadenze e cedole, si può per ognuno di essi calcolare il corrispondente rendimento a scadenza $R(t,s)$, in questo modo si avrà un insieme di coppie ordine, in cui l'ascissa è data dalla scadenza e l'ordinata dal relativo rendimento, la curva che se ne ottiene prende il nome di curva dei rendimenti.

Il modello di Nelson-Siegel-Svensson

Date le relazioni che sussistono tra la funzione di sconto $P(t,s)$, il rendimento a scadenza $R(t,s)$ e l'intensità istantanea d'interesse $f(t,s)$, parleremo di modelli *cross-sectional* quando si stabilisce una forma funzionale rispetto alla variabile s per una di queste funzioni. L'idea è quella di postulare una forma funzionale per la funzione da stimare che può essere data da una famiglia specifica di funzioni dipendenti da un vettore di parametri. Il problema della stima della relativa curva dei rendimenti è quindi ridotto alla stima del vettore dei parametri dai dati di mercato.
Una classe di modelli particolarmente utilizzata è costituita dai modelli parsimoniosi. L'idea di base di questa classe di modelli, è quella di imporre a priori alcune proprietà e contemporaneamente di limitare il numero dei parametri che determinano la forma funzionale. Tali parametri devono essere quindi stimati a partire dalle quantità osservate.
Ai fini del presente contributo si illustreranno i modello proposto da Nelson - Siegel in [NS] e l'estensione di quest'ultimo proposta da Svensson in [S].
Il modello di Nelson - Siegel (NS) assume che l'intensità istantanea d'interesse $f(t,s)$ è la soluzione dell'equazione

$$f(t,s)=\beta_0+\beta_1\cdot\exp\left(\frac{t-s}{\tau}\right)+\beta_2\cdot\frac{s-t}{\tau}\cdot\exp\left(\frac{t-s}{\tau}\right) \qquad (6)$$

Questa equazione genera una famiglia di curve in cui monotonia, curvatura e forma dipendono dai valori di β_1, β_2 e τ ed ha un asintoto in β_0.
Il rendimento a scadenza $R(t,s)$ è dato da

$$R(t,s)=\frac{1}{s-t}\int_t^s f(t,u)du$$

da cui si ottiene integrando $R(t,\bullet)$ tra t e s e dividendo per $(s-t)$ si ottiene

$$R(t,s) = \beta_0 + (\beta_1 + \beta_2)\cdot\left(1 - \exp\left(\frac{t-s}{\tau}\right)\right)\cdot\frac{\tau}{s-t} - \beta_2\cdot\exp\left(\frac{t-s}{\tau}\right) \qquad (7)$$

Se si pone $\tau = 1$, $\beta_0 = 1$, $(\beta_0 + \beta_1) = 0$ e $\beta_2 = a$ la (7) diviene

$$R(t,s) = 1 - (1-a)\cdot(1 - \exp(t-s))/(s-t) - a\cdot\exp(t-s)$$

Al variare del parametro a con incrementi costanti da -6 a +6 si ottengono le diverse forme di curve del rendimento a scadenza (gobbe, curve ad U, forme ad s e curve monotone) come si evince dalla figura 1.

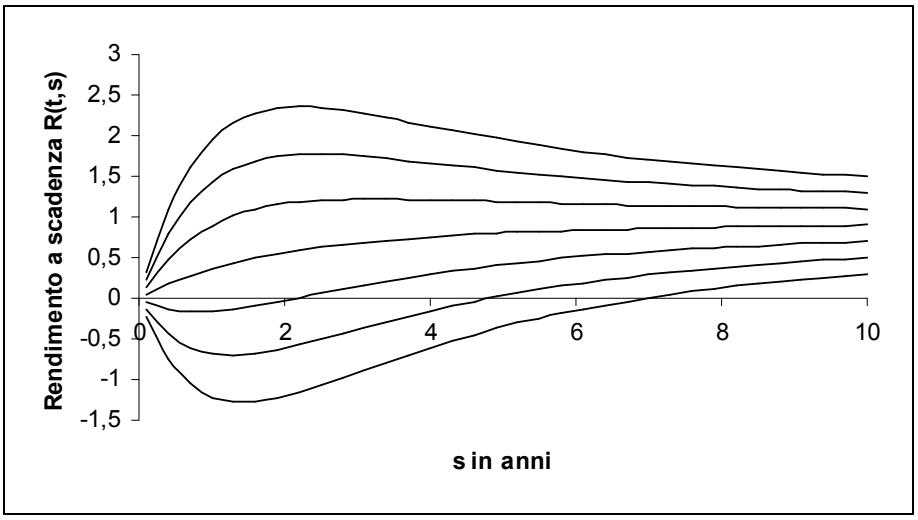


Figura 1

I coefficenti del modello misurano le forze delle componenti del breve, medio e lungo termine, infatti, il contributo del lungo termine è determinato da β_0, quello del breve termine da β_1, mentre β_2 indica il contributo della componente del medio termine. La componente del lungo termine è una costante che non tende a zero in limite.
La curva del medio termine è la sola nel modello che parte da zero e tende a zero. La curva del breve termine non parte da zero e tende a zero ed è quella che decade più velocemente, come si evince dalla figura 2, in cui si è posto $\beta_0 = 0{,}07$; $\beta_1 = 0{,}05$; $\beta_2 = 0{,}12$ e $\tau = 1$;

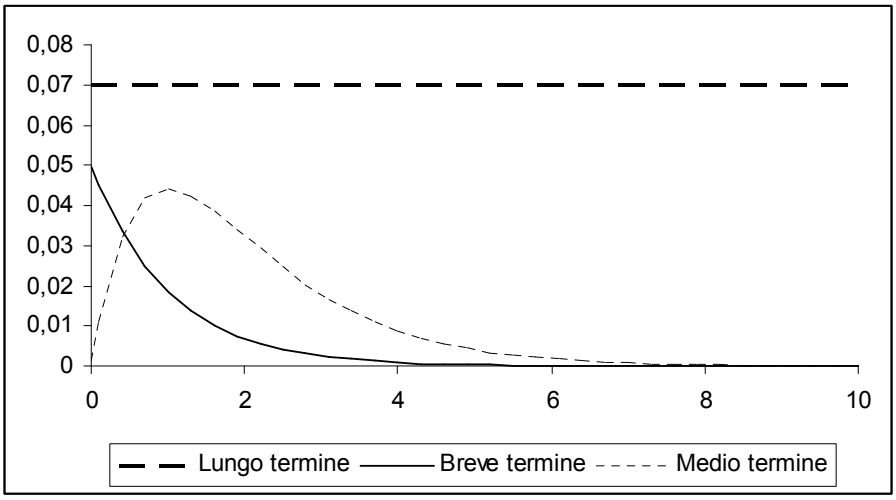


Figura 2 Componenti dell'intensità istantanea d'interesse

E' facile notare che scegliendo appropriatamente i pesi di queste componenti si possano generare diverse curve dei rendimenti basate sul tasso.
Per incrementare la flessibilità e migliorare l'adattamento Svensson in [S] estende la funzione di Nelson - Sigiel (6) aggiungendo un quarto termine

$$\beta_3 \cdot \frac{s-t}{\tau_2} \cdot \exp\left(\frac{t-s}{\tau_2}\right)$$

che genera una seconda gobba (o una forma ad U) con due nuovi parametri β_3 e τ_2. Il comportamento di questa nuova componente è del tutto simile alla componente del medio termine di NS con β_3 e τ_2 al posto di β_2 e τ. Nel modello di Nelson – Siegel - Svensson (NSS) la struttura per scadenza delle intensità istantanea di interesse al tempo t è definita dalla funzione

$$f(t,s) = \beta_0 + \beta_1 \cdot \exp\left(\frac{t-s}{\tau_1}\right) + \beta_2 \cdot \frac{s-t}{\tau_1} \cdot \exp\left(\frac{t-s}{\tau_1}\right) + \beta_3 \cdot \frac{s-t}{\tau_2} \cdot \exp\left(\frac{t-s}{\tau_2}\right) \qquad (8)$$

definita per $(s-t) \geq 0$ e dove β_0, β_1, β_2, β_3, τ_1 e τ_2 sono parametri reali che soddisfano i vincoli di significatività

$$\beta_0 > 0 \qquad \beta_0 + \beta_1 > 0 \qquad \tau_1 > 0 \qquad \tau_2 > 0 \qquad (9)$$

Il modello NSS può essere riscritto come somma di quattro componenti

$$f(t,s) = f_0(t,s) + f_1(t,s) + f_2(t,s) + f_3(t,s)$$

Pertanto, la curva del modello è la risultante della somma delle quattro componenti.
I parametri dipendono dalla data t di contrattazione ed il modello non fa nessuna ipotesi di dipendenza da t, ovvero sulla sua dinamica, in questo senso è un modello statico, infatti descrive solo la struttura per scadenza al tempo t. Inoltre, il modello non dipende da s, ma solo dalla differenza tra t e s.
La struttura per scadenza del rendimento a scadenza al tempo t è definita dalla funzione

$$R(t,s) = \frac{1}{s-t}\int_t^s f(t,u)du$$

ovvero

$$R(t,s) = \beta_0 + \tau_1 \cdot \beta_1 \cdot \left(1 - \exp\frac{t-s}{\tau_1}\right)/(s-t) +$$

$$+ \beta_2 \cdot \left[\tau_1\left(1 - \exp\left(\frac{t-s}{\tau_1}\right)\right)/(s-t) - \exp\left(\frac{t-s}{\tau_1}\right)\right]$$

$$+ \beta_3 \cdot \left[\tau_2 \cdot \left((1 - \exp\left(\frac{t-s}{\tau_2}\right)\right)/(s-t)\right] - \exp\left(\frac{t-s}{\tau_2}\right)\right] \qquad (10)$$

La struttura per scadenza del tasso d'interesse a pronti al tempo t è definita dalla funzione

$$i(t,s) = \exp(R(t,s)) - 1$$

La funzione di sconto è definita da

$$P(t,s) = \exp((s-t) \cdot R(t,s)) \qquad (11)$$

La curva dei rendimenti della BCE

La Banca Centrale Europea utilizza il modello di NSS per la stima delle curve dei rendimenti riferite all'euro mercato.
La BCE pubblica giornalmente sul suo sito le curve dei rendimenti stimate con il metodo di NSS dal 6 settembre 2004, calcolate a partire dalle quotazioni sull'Euro MTS (Mercato dei Titoli di Stato). La BCE stima quotidianamente a fine giornata due curve dell'area euro. Quella principale è stimata sui prezzi di titoli di Stato con rating (Fitch) AAA, che assume il significato della struttura per scadenza *risk-free* dell'area euro. Un'altra curva è calcolata a partire dai prezzi di tutti i titoli di Stato dell'area euro.
In entrambi i casi vengono considerati solo titoli denominati in euro, con poste deterministiche (titoli senza cedola e titoli con cedola fissa), *maturity* da 3 mesi a 30 anni, nominale emesso di almeno 5 miliardi di euro ed effettivamente scambiati nella giornata.

La calibrazione dei parametri

Per calibrare i parametri del modello la BCE in una generica data t procede nel seguente modo:

1. reperisce dal mercato i prezzi dei titoli quotati a fine giornata con le caratteristiche precedentemente specificate e li classifica per maturity;
2. assume che i tassi d'interesse seguano una forma funzionale i cui parametri le consentono di essere sufficientemente duttili;
3. calibra i parametri della forma funzionale (modello) in modo da renderla il più aderente possibile ai dati reperiti dal mercato;
4. ottiene i dati mancanti utilizzando la forma funzionale stimata.

Quindi, alla data di riferimento t, si considerano n titoli x_j, con $j=1,2,.....n$ con prezzo P_j con $j=1,2,.....n$ che generano ciascuno un proprio flusso $\{c_{j1},c_{j2},.....,c_{jm}+C_j\}$ su uno scadenzario comune $\{t_1,t_2,.....,t_m\}$. Il prezzo stimato $\overline{P}_j$ del j-titolo utilizzando la (2) al tempo t è

$$\overline{P}_j = c_{j1}\cdot P_\omega(t,t_1)+c_{j2}\cdot P_\omega(t,t_2)+.....+(c_{jm}+C_j)\cdot P_\omega(t,t_m)$$

dove $P_\omega(t,t_k)$ con $k=1,2,.....m$ è il fattore di sconto tra il tempo t ed il tempo t_k definito dalla (11) e dipendente dal parametro ω.
La metodologia per la calibrazione dei parametri del modello di NSS prevede che il vettore $\omega=\{\beta_0,\beta_1,\beta_2,\beta_3,\tau_1,\tau_2\}$ dei parametri stimati degli n titoli sia la soluzione del problema di ottimizzazione vincolata

$$\min_{\omega\in\Omega}\sum_{j=1}^{n}(P_j-\overline{P}_j)^2$$

dove Ω è l'insieme dei vettori che soddisfano i vincoli di significatività (9).

Nella figura 3 sono riportati i grafici su base annua dell'intensità istantanea $f(t,s)$, del rendimento a scadenza $R(t,s)$ e dei tassi a pronti $i(t,s)$ stimati dalla BCE del 28/02/2011, il tempo è espresso in anni con i seguenti valori dei parametri: $\beta_0 = 1{,}605537\%$, $\beta_1 = -1{,}048783\%$, $\beta_2 = 13{,}387869\%$, $\beta_3 = -4{,}068860\%$, $\tau_1 = 9{,}260119$ e $\tau_2 = 9{,}068778$.

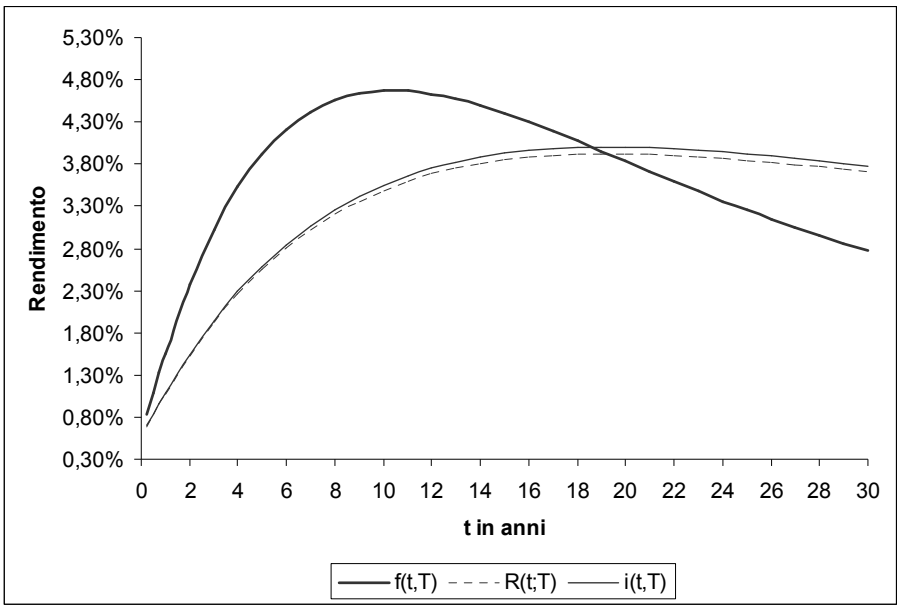


Figura 3 Struttura per scadenza risk- free stimata dalla BCE il 28/02/2011

Nella figura 4 sono riportati i grafici delle quattro componenti dell'intensità istantanea $f(t,s)$ risk- free stimata dalla BCE il 28/02/2011

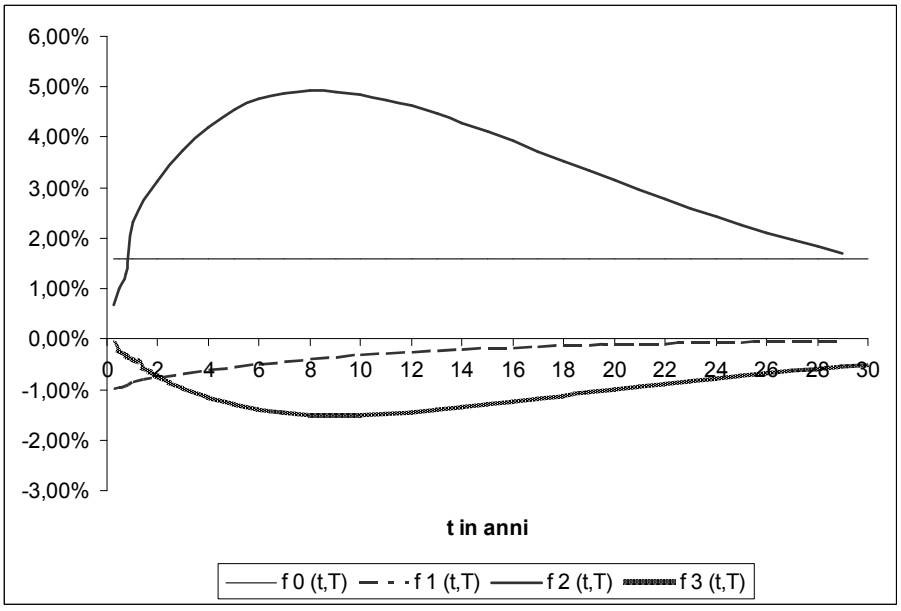


Figura 4 Componenti dell'intensità istantanea d'interesse risk- free stimata dalla BCE il 28/02/2011.

Bibliografia

[ADGS] Anzilli L., D'Agostino G., Guglielmi A., Scolozzi D., *Liability Management negli Enti Locali.*Trepuzzi (LE), Edizioni Publigrafic, pp. 1-128, ISBN 8890226641.

[BCE] BCE *Techical notes.*
http://www.ecb.europa.eu/stats/money/yc/html/technical_notes.pdf

[CIR] Cox, J.C., Ingersoll, J.E., Ross, S.A. *A Theory of the Term Structure of Interest Rate.* In Econometrica, 53, pp. 385-407, 1985.

[H] Hull, J. C. *Option, futures ed altri derivati.* Prentice - Hall International, 2000.

[M] Moriconi, F. *Matematica finanziaria.* Bologna, Il Mulino, 1995.

[NS] Nelson, C. R., Siegel, A. (1987) *A Parsimonious Modelling of Yield Curves.* Journal of Business, vol. 60, n. 4, pp. 473-489.

[S] Svensson, L.E.O., (1994) *Estimating and interpreting forward interest rates: Sweden 1992-1994*, IMF Working Paper, n. 114.

[V] Vasicek, O. (1977) *An equilibrium characterization of the term structure*, Journal of Financial Economics, 5, pp. 177-188.

152. Tre congetture di P. Erdös

di Andreana Zucco

Sunto

Vengono esaminate tre congetture di P. Erdös riguardanti insiemi composti da un numero finito di punti nel piano. Nella prima dati n punti si considerano le distanze determinate dalle coppie di punti della configurazione e si cerca di disporli in modo che il numero delle distanze sia minimo. Nella seconda si cerca tale minimo nel caso in cui i punti siano i vertici di un poligono convesso. Infine nella terza il problema è trovare una configurazione di n punti in cui una distanza appaia una sola volta, una si ripeta 2 volte, una si ripeta 3 volte, ..., una si ripeta (n-1) volte; il motivo di questo curioso quesito geometrico deriva da un'uguaglianza algebrica.

Incontrai Paul Erdös ad un convegno di Geometria Convessa a Dortmund, nel 1991. Per i partecipanti la cena, molto informale, era a casa di Tudor Zamfirescu, organizzatore del convegno. Durante la cena non osavo parlargli, dato il mio stentato inglese, per cui feci fare ad un altro la mia domanda un po' banale: Quanti lavori ha pubblicato? - Non conoscevo il numero preciso, ma sapevo che erano più di mille.
La risposta fu: - Troppi.
Un grande matematico e anche un grande critico di se stesso.
Le sue congetture nascevano da semplici e acute considerazioni, qui ne illustreremo alcune.

I

Consideriamo n punti nel piano $x_1, x_2,\ldots, x_n$ e indichiamo con $d(x_1, x_2,\ldots, x_n)$ il numero delle distanze diverse fra loro. Tutte le possibili distanze che si possono ottenere sono le combinazioni di n punti a 2 a 2. Quindi in tutto sono $\frac{n(n-1)}{2}$ (vedi ad esempio F. Cimolin, *Il Coefficiente Binomiale*, su questo sito) per cui

$$d(x_1, x_2,\ldots, x_n) \leq \frac{n(n-1)}{2}$$

Per esempio supponiamo n=3 e che i tre punti x_1, x_2, x_3 siano i vertici di un triangolo:

- se è scaleno $d(x_1, x_2, x_3)=3$,
- se è isoscele $d(x_1, x_2, x_3)=2$,
- se è equilatero $d(x_1, x_2, x_3)=1$.

Se i tre punti distinti sono allineati, si ha $d(x_1, x_2, x_3)=2$ se x_2 è il punto medio del segmento $[x_1, x_3]$, in caso contrario $d(x_1, x_2, x_3)=3$.
Si può quindi considerare il numero minimo delle diverse distanze $d(x_1, x_2,\ldots, x_n)$ al variare della configurazione dei punti e indicarlo con

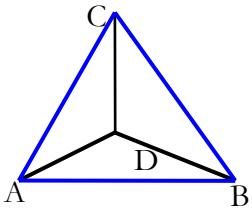
$$f(n) = \min d(x_1, x_2,\ldots, x_n) .$$

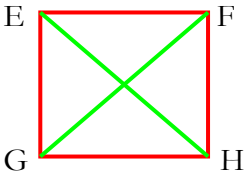
Nel caso precedente si ha

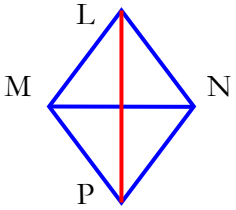
$$f(3)=1.$$

Per costruire un altro esempio, consideriamo per n=4 i seguenti casi:

- i punti sono i vertici di un triangolo equilatero ed il suo centro, in tal caso si hanno 2 diverse misure: il lato e la distanza del centro da un vertice;
- i punti sono i vertici di un quadrato, le misure diverse sono 2 la misura dei lati e la misura delle diagonali;
- i punti sono i vertici di un rombo dato da due triangoli equilateri incollati lungo un lato, come misure diverse si ha il lato e la diagonale maggiore.







Nei tre casi $d(x_1, x_2, x_3, x_4)=2$. Poiché si dimostra facilmente che $d(x_1, x_2, x_3, x_4) \neq 1$, si ha $f(4)=2$.
Pensare di determinare f(n) per qualsiasi n, è un problema posto da P. Erdös nel 1946 che egli stesso ha definito "hopeless": infatti a cominciare da Erdös stesso, ci sono stati diversi tentativi, ma tutti volti solo ad una stima del possibile valore di f(n). Fra l'altro egli ha provato (vedi [2]) che

$$f(n)>\sqrt{n-1}\ -1$$

e tale disuguaglianza vale nei casi visti

$$\sqrt{2}\ -1 < f(3)=1\ ; \qquad \sqrt{3}\ -1 < f(4)=2.$$

L. Moser nel 1952 (vedi [7]) ha migliorato tale risultato, dimostrando che

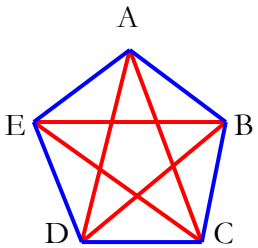
$$f(n)>\frac{\sqrt[3]{n^2}}{2\sqrt[3]{9}}$$

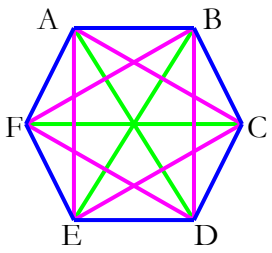
che per n>5184 è un risultato migliore del precedente.
In seguito ci sono stati ancora altri studiosi che hanno dato almeno parzialmente una risposta a questo problema.

II

Invece di considerare una configurazione qualsiasi, ora pensiamo gli n punti come vertici di un poligono convesso.

- Se n=5 ed il pentagono è regolare si ha f(5)=2, le due diverse misure sono quelle del lato e della diagonale,
- se n=6 e l'esagono è regolare si ha f(6)=3, le tre diverse misure sono il lato e le due diagonali,
- se n=7 e l'ettagono è regolare si ha f(7)=3, come nel caso precedente misure diverse sono date dal lato e da due diagonali, ecc.



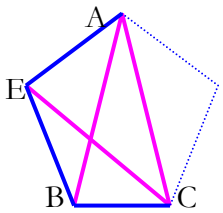


Da simili osservazioni Erdös aveva congetturato che nel caso in cui gli n punti coincidessero con i vertici di un poligono convesso, f(n) sarebbe risultato maggiore od uguale alla parte intera di $\frac{n}{2}$:

$$f(n)\geq[\frac{n}{2}]$$

e l'uguaglianza sarebbe valsa nel caso in cui il poligono fosse regolare.

A provare che la congettura era vera riuscì E. Altman nel 1963, con una complessa dimostrazione. Egli provò che ogni poligono convesso include almeno $\left[\frac{n}{2}\right]$ differenti distanze fra le corrispondenti coppie di vertici, anzi precisò pure che un poligono convesso con un numero dispari di vertici n=2N+1 ha esattamente N diverse distanze se e solo se è un poligono regolare.
Quindi se ho 5 punti ed f(5)=2 certamente il pentagono è regolare.
Nel caso in cui i punti siano in numero pari n=2N, si ha f(2N)=N in due casi: se il 2N-poligono è regolare oppure se il poligono è costruito a partire da un (2N+1)-poligono regolare meno un punto.
Quindi se ho 4 punti e f(4)=2 i punti possono essere i vertici di un quadrato, come già detto, oppure i vertici di un poligono ottenuto da un pentagono regolare meno un punto.

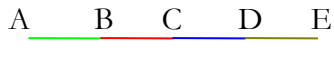


III

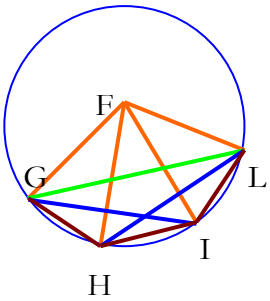
Fra i problemi collegati alle distanze di n punti, è particolarmente degno di nota quello che trae spunto dalla seguente uguaglianza numerica.

Le distanze di n punti sono in tutto le combinazioni di n punti a 2 a 2 ossia sono $\frac{n(n-1)}{2}$, ma anche 1+2+….+(n-1) vale $\frac{n(n-1)}{2}$.

Prendendo spunto da questa uguaglianza Erdös ebbe l'idea del seguente problema: è possibile trovare una configurazione di n punti che soddisfi alla condizione che la somma totale delle distanze sia data da una distanza che si presenti una sola volta, una che si ripeta 2 volte, una che si ripeta 3 volte, .., una che si ripeta (n-1) volte? Per evitare casi banali aggiunse che nella configurazione non dovevano esserci 3 punti allineati e neppure 4 su un cerchio.
Per esempio, per n=5 troviamo le due seguenti configurazioni che non devono essere considerate, dato che sono facilmente estendibili per valori maggiori di n con la stessa tecnica.



AB=BC=CD=DE
AC=CE=BD
AD=BE
AE



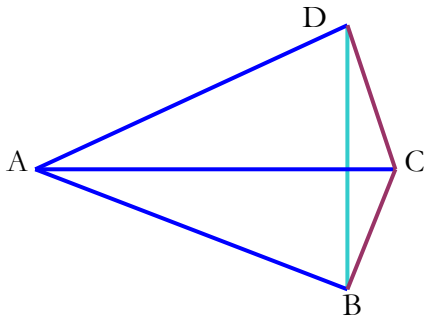
FG=FH=FI=FL
GH=HI=IL
GI=HL
GL

Mentre per n=5 una costruzione valida è ad esempio quella fatta da C. Pomerance, che illustreremo dopo.
Erdös pensava che esistesse un numero n_0 abbastanza grande, tale che per ogni numero $n > n_0$ non si trovassero configurazioni alle condizioni poste. Tanto è vero che offrì 50 dollari a chi fosse riuscito a

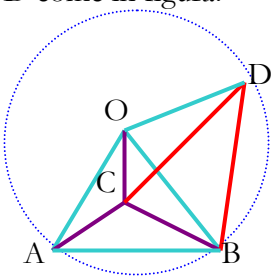
dimostrare questa congettura e 500 dollari a chi fosse riuscito a trovare degli esempi per n abbastanza grande.
Chi trovò i risultati migliori fu Ilona Palàsti, che trovò configurazioni che rispettavano le condizioni richieste con 5,6,7 fino a 8 punti.
Qui daremo solo qualche esempio per valori di n ≤6.

Per n=3 basta considerare un triangolo isoscele non equilatero A,B,C di base AC. Si ha AB=BC di molteplicità 2 e poiché non è equilatero tale distanza è diversa da AC di molteplicità 1.

Per n=4 consideriamo un punto A centro di una circonferenza di raggio 1. Su di essa consideriamo tre punti B,C,D in modo che BC=CD e BC sia diverso da 1. Indichiamo con α l'angolo BAC= all'angolo CAD. Se $\alpha \neq 60^o$ e $\alpha \neq 30^o$ si hanno 6 distanze tali che:
AB=AC=AD=1 è una distanza di molteplicità 3
BC=CD=$\sqrt{2(1-\cos a)}$ (per il teorema di Carnot) è una distanza di molteplicità 2
BD=2sen α è una distanza di molteplicità 1.
Inoltre ovviamente 3 punti non sono allineati e 4 non stanno su un cerchio, perché il cerchio che passa per B,C,D non passa per A, avendo centro in A.



Per n=5 seguendo C. Pomerance, consideriamo un cerchio di centro O e siano A e B due punti sulla circonferenza, tali che il triangolo OAB sia equilatero. Come quarto punto C consideriamo il centro di tale triangolo. Infine consideriamo l'asse di uno dei tre segmenti CA,CB,CO, per esempio CB; l'asse interseca la circonferenza in un punto D come in figura.



L'insieme dei punti {O,A,B,C,D}soddisfa alle condizioni richieste. Notiamo che
AO=OB=AB=OD è di molteplicità 4,
AC=CO=CB (ove AO≠AC) è di molteplicità 3,
CD=DB è di molteplicità 2
e la distanza AD è unica.
Dalla figura si vede che 3 punti non sono allineati e si prova che 4 non stanno su un cerchio.

Per n=6 per considerare un esempio di I. Palàsti, introduciamo nel piano un sistema di riferimento cartesiano e ricordiamo che dati due punti P_1 di coordinate (x_1,y_1) e P_2 di coordinate (x_2,y_2) la loro distanza è data da $\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}$. I sei punti dell'esempio hanno coordinate

A(3, $3\sqrt{3}$) B(0, 0) C(6, 0) O'(3, $\sqrt{3}$) A'(-$2\sqrt{6}$, $2\sqrt{3}$) B'(3+$\sqrt{6}$, -$\sqrt{3}$ -$3\sqrt{2}$).

Con la formula della distanza si verifica che

AB=AC=BC=BA'=CB' è di molteplicità 5

AA'=BB'=O'A'=O'B' è di molteplicità 4

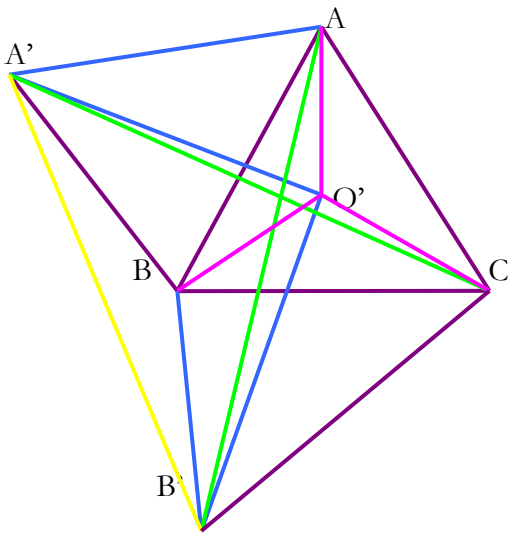
AO'=BO'=CO' è di molteplicità 3

AB'=CA' è di molteplicità 2

A'B' è di molteplicità 1.

Inoltre con la geometria analitica si verifica che non ci sono tre punti su una retta, né quattro su un cerchio.

Unendo i punti si ottiene la figura cercata.



Per chi vuole approfondire l'argomento, può consultare i lavori di Ilona Palàsti citati nella bibliografia.

Bibliografia

[1] E. Altman, *On a problem of P. Erdös*, Amer.Math.Montly, n.70 (1963) 148-157.
[2] P. Erdös, *On sets of distances of n points*, Amer.Math.Montly, n.53 (1946) 248-250.
[3] P. Erdös, *On sets of distances of n points*, Amer.Math.Montly, n.77 (1970) 738-740.
[4] P. Erdös, *Distances with Specified Multiplicities*, Amer.Math.Montly, n.96 (1989) 447.
[5] P. Erdös, G.Purdy, *Estremal Problems in Combinatorial Geometry*, Handbook of Combinatorics Edit by R.Graham, M. Grötschel and L.Lovàsz (1995).
[6] A.Liu, *On the "Seven points problem" of P. Erdös*, Math.Chronicle, n.15 (1986) 29-33.
[7] L.Moser, *On the different distances determined by n points*, Amer.Math.Montly, n.59 (1952) 85-91 .
[8] I.Palàsti, *On the seven points problem of P. Erdös*, Studia-Sci.-Math.-Hungar., n.22 (1987) 447-448.
[9] I.Palàsti, *A distance problem of P. Erdös with some further restrictions*, Discrete-Math., n.76 (1989) 155-156.
[10] I.Palàsti, *Lattice point examples for a question of P. Erdös*, Studia-Sci.-Math.-Hungar., n.20 (1989) 231-235.
[11] I.Palàsti, *On some distances properties of sets of points in general position in space*, Studia-Sci.-Math.-Hungar., n.24 (1989) 187-190.

153. Dai Numeri Primi alla Crittografia

Gianluca Salvalaggio
gianluca.salvalaggio@gmail.com

Per secoli il fascino dei numeri primi ha catturato l'interesse dei più grandi matematici. Le proprietà di questi eleganti oggetti sono state a lungo esplorate e in questi ultimi decenni, con l'evoluzione delle tecnologie informatiche, hanno trovato estese applicazioni nell'ambito della cosiddetta Crittografia a chiave pubblica.
Nelle pagine che seguono cercheremo di capire quali profonde problematiche si celano dietro la bellezza dei numeri primi e comprenderemo come essi vengono applicati nelle moderne tecniche crittografiche. In particolare verrà analizzato l'algoritmo di cifratura RSA che sfrutta, con ingegnosa semplicità, la difficoltà di scomporre in fattori primi un numero N molto grande.

1. Numeri primi

I concetti di numero naturale e di numero intero ci sono ben familiari. I numeri naturali sono quelli che si impararano da bambini e che quotidianamente utilizziamo per *contare le cose* ("*… 44 gatti in fila per 6 col resto di 2 …*"). I numeri interi invece vengono informalmente definiti come l'unione dei numeri naturali e dei "numeri con segno" (detti anche numeri relativi). Se quindi indichiamo con $\mathbf{N}$ e $\mathbf{Z}$ rispettivamente l'insieme dei numeri naturali e dei numeri interi, possiamo scrivere:

$$\mathbf{N} = \{ 0, 1, 2, 3, \dots \}$$

$$\mathbf{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$$

Una peculiarità che accomuna i numeri naturali ed i numeri interi è il concetto di divisibilità. Dati i numeri interi m e n, si dice che ***n* divide *m***, e si scrive $n \mid m$, se esiste un intero k tale che $m = nk$. Sia n che k vengono detti divisori (o fattori) di m.
Altresì, dati due numeri m_1 e m_2, si definisce **massimo comun divisore** (*greatest common divisor*), e si indica con $\gcd(m_1, m_2)$, il più grande intero che divide sia m_1 che m_2.
Ad esempio $\gcd(6,8) = 2$, mentre $\gcd(12,4) = 4$.
Siamo in grado, quindi, di definire cos'è un **numero primo**:

"un numero intero m si dice primo se è divisibile solo per se stesso e per 1"

Più semplice di così: i numeri primi non ammettono divisori diversi da loro stessi e da 1.
Alcuni esempi sono: 2, 3, 5, 7, 11, 13, 17, 19, … 53, ..., 101, ….
Viceversa, i numeri interi che non sono primi vengono detti **compositi**, proprio perché possono essere espressi come prodotto di due o più numeri. Ad esempio 6 è esprimibile come $2 \cdot 3$.
Una proprietà un po' più *debole*, e che non riguarda un singolo numero ma una coppia di numeri è la **coprimalità**:

"due numeri m ed n sono coprimi, o primi relativi, se vale $\gcd(m,n) = 1$"

Ad esempio i numeri 8 e 9 presi singolarmente sono tutt'altro che primi ma, come si può facilmente verificare, sono coprimi perché vale $\gcd(8,9) = 1$.

2. Conoscere i numeri primi

Bene, introdotte le doverose definizioni possiamo affrontare alcuni quesiti che riguardano i numeri primi.

- anzitutto, perché sono così importanti?
- sono finiti o infiniti?
- siamo in grado di contarli?

Andiamo con ordine: chiariamo perché è importante studiare i numeri primi.
Si può dire che i numeri primi rappresentano i "mattoni elementari", gli atomi, con cui costruire, attraverso l'operazione di moltiplicazione, tutti gli altri numeri interi. Tale concetto è ben formalizzato nel noto:

Teorema Fondamentale dell'Aritmetica. Ogni intero positivo N o è primo oppure è esprimibile come prodotto di numeri primi, e tale fattorizzazione è unica.
Cosa significa? Significa che preso un qualunque numero naturale, ad esempio 12, esso può essere espresso come prodotto di due o più numeri primi, e tale rappresentazione è unica. Infatti 12 è rappresentabile come il prodotto: $2 \cdot 2 \cdot 3$. Ovviamente se il numero considerato è già primo, ad esempio 7, la sua fattorizzazione è banale.

Al secondo quesito (*sono finiti o infiniti?*) rispose per primo Euclide, dimostrando il seguente:

Teorema sull'Infinità dei numeri primi (Euclide). Esistono infiniti numeri primi.
Dimostrazione. Supponiamo per assurdo che i numeri primi siano in numero finito, diciamo k:
$p_1, p_2, p_3, \ldots, p_i, \ldots p_k$. Consideriamo quindi i numeri $P = p_1 p_2 \cdots p_k$ ed $N = P + 1$. Siccome vale $N > p_k$, il numero N non può essere primo (sarebbe in contraddizione con le ipotesi), quindi deve ammettere dei fattori primi. D'altra parte N non risulta divisibile per nessuno dei primi p_i considerati. Se così fosse, infatti, si avrebbe che p_i divide sia P (per costruzione) che $N = P + 1$, e quindi dividerebbe anche la loro differenza cioè $(P + 1) – P = 1$. Assurdo

Ricapitolando quindi, i numeri primi sono infiniti e per mezzo di loro possiamo esprimere tutti i numeri naturali. A questo punto è lecito chiedersi se siamo in grado di calcolarli o quanto meno di determinare quanti sono i numeri primi minori di un certo valore n.
Queste problematiche sono state affrontate già ai tempi degli antichi Greci, come testimonia il seguente procedimento, attribuito ad Eratostene (III° secolo a.C.)

Crivello di Eratostene. Si tratta di un metodo veloce per determinare i numeri primi minori di una certa quantità n.
L'algoritmo parte dal presupposto che, dato un numero n, il suo più piccolo fattore primo è sempre minore o uguale a $\sqrt{n}$. La cosa è facilmente dimostrabile: sia p il più piccolo fattore primo di n, quindi si può scrivere $n = pd$, con $d \geq p$. Pertanto $n = pd \geq pp = p^2 \Rightarrow p \leq \sqrt{n}$.
Ad esempio, dato $n = 35 = 5 \cdot 7$ si verifica facilmente che 5 è minore di $\sqrt{35}$.
Il Crivello calcola i numeri primi minori di n nel modo seguente:

a. elenchiamo tutti i numeri compresi fra 2 ed n
b. eliminiamo tutti i multipli di 2
c. il più piccolo numero maggiore di 2 "sopravissuto" all'eliminazione precedente è 3: quindi eliminiamo tutti i multipli di 3.
d. si continua così, eliminando i multipli di 5 e poi di 7 etc. etc., fino ad arrivare a $\sqrt{n}$
e. i numeri "sopravissuti" alla selezione (2, 3, 5, …) sono i primi $\leq n$.

3. Il Teorema dei Numeri Primi

La tecnica di Eratostene è semplice, concettualmente chiara, ma impraticabile per valori di n molto grandi. Nei secoli a venire, peraltro, gli sforzi dei matematici si sono concentrati nel cercare di capire se vi è una qualche regolarità nell'infinita successione dei primi. La loro distribuzione, in effetti, appare incostante, imprevedibile, quasi bizzarra. Ad esempio tra 10 e 20 vi sono ben 4 numeri primi, mentre fra 800 e 820 ce ne sono soltanto 2. Vi sono poi i cosiddetti numeri **primi gemelli**, ossia coppie di numeri primi che differiscono fra loro di 2 (ad esempio le coppie 11 e 13, 107 e 109). E' facile dimostrare inoltre che si possono trovare numeri primi consecutivi a distanza arbitrariamente grande, ossia [1, p. 38]:

Teorema. Sia $k > 1$ un intero qualunque, allora esistono k numeri naturali consecutivi nessuno dei quali è primo.

D'altra parte già nel 1845 il matematico francese Joseph Bertrand formulò l'omonima congettura (dimostrata cinque anni più tardi da Chebyshev):

Postulato di Bertrand. Per ogni intero $n > 1$ c'è sempre un numero primo compreso fra n e $2n$.

In definitiva risultava chiaro che uno dei grandi problemi legato ai numeri primi era quello di capire in che modo essi si susseguono. Una misura di questa comprensione viene epressa dalla funzione *conta-primi* $\pi(x)$ così definita:

$$\pi(x) = \text{n° dei primi } \leq x$$

Ad esempio, $\pi(10) = 4$ (i numeri primi ≤ 10 sono 2,3,5,7), $\pi(30) = 10$ e così via.
Il fatto che i numeri primi sono infiniti quindi, può essere riformulato nel modo seguente:

$$\lim_{x \to +\infty} \pi(x) = +\infty$$

Tra i vari matematici che hanno studiato la funzione $\pi(x)$, vi è senz'altro Carl Friedrich Gauss, considerato da molti il *Principe dei Matematici*. Sulla base di risultati numerici egli congetturò, nel 1792 a soli 15 anni, che $\pi(x)$ tende asintoticamente alla funzione $\frac{x}{\log x}$ per $x \to +\infty$ ($\log x$ rappresenta il logaritmo di x in base e). Cioè che per valori via via più grandi di x le funzioni $\pi(x)$ e $\frac{x}{\log x}$ assumono valori sempre più vicini (in proporzione). Sinteticamente:

$$\pi(x) \sim \frac{x}{\log x}$$

In realtà né Gauss né i suoi contemporanei riuscirono a dimostrare questa corretta intuizione. Infatti, nonostante i successivi progressi effettuati dal russo Chebyshev nella direzione di una dimostrazione rigorosa, si dovette aspettare più di un secolo affinchè, nel 1896, due eminenti matematici, Jacques Hadamard e Charles-Jean De la Vallèe-Poussin, dimostrarono, in modo indipendente, quello che è universalmente conosciuto come il

Teorema dei Numeri Primi. $\pi(x)$ è asintotica alla funzione $\frac{x}{\log x}$, ossia vale:

$$\lim_{x \to +\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

4. La funzione Zeta di Riemann

Nelle rispettive dimostrazioni, sia Hadamard che De la Vallèe-Poussin utilizzarono avanzate tecniche di calcolo legate alla Teoria Analitica dei Numeri, ossia quel ramo della matematica che coniuga la Teoria dei Numeri con l'Analisi Complessa. In particolare attinsero ai preziosi risultati ottenuti, qualche decennio prima, dal grande matematico Bernard Riemann.

Questi infatti, nel suo celebre articolo del 1859 dal titolo "*Sul* numero di primi minori di una grandezza data"[1], approcciò lo studio della funzione $\pi(x)$ utilizzando metodi di analisi complessa. Più precisamente egli considerò la funzione Zeta $\zeta(s)$, definita dal Prodotto di Eulero, come una funzione di variabile complessa (tecnicamente parlando effettuò un prolungamento analitico della funzione $\zeta(s)$).

Una cosa alla volta: cos'è la funzione Zeta $\zeta(s)$ e cosa si intende per Prodotto di Eulero?

Il tutto iniziò verso il 1740 quando il matematico svizzero Eulero, uno dei più prolifici della storia, introdusse la funzione **Zeta** $\zeta(x)$ definita, per tutti i numeri reali $x > 1$, dalla somma infinita (serie):

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \cdots = \sum_{n=1}^{+\infty} \frac{1}{n^x}$$

Per $x \le 1$ la somma dà un risultato infinito (la serie diverge) mentre per $x > 1$ la somma ritorna un valore finito (la serie converge). Eulerò dimostrò che per tali valori di x vale l'identità:

$$\zeta(x) = \sum_{n=1}^{+\infty} \frac{1}{n^x} = \prod_{p \in \mathrm{P}} \frac{1}{1 - p^{-x}}$$

nota appunto come **Prodotto di Eulero**.

La cosa sorprendente di questa identità è che il prodotto a destra è esteso a tutti i numeri primi (con P infatti si intende l'insieme di tutti i numeri primi), a conferma della natura "fondamentale" di questi ultimi.

Riemann ebbe il merito di estendere la funzione Zeta al campo dei Complessi (numeri nella forma $s = a + ib$, con $i = \sqrt{-1}$), ottenendo l'omonima **Funzione Zeta** $\zeta(s)$. Il procedimento utilizzato fu appunto quello del *prolungamento analitico* (la cui comprensione va oltre gli scopi del presente articolo) e ciò gli permise di ottenere una funzione definita su tutto il piano complesso.

L'importanza del contributo di Riemann è dovuta al fatto che vi è uno stretto legame fra la funzione $\pi(x)$ e la funzione Zeta $\zeta(s)$. Sempre in quell'articolo il matematico tedesco formulò, senza darle particolare importanza, una congettura la cui dimostrazione è ancora oggi tra i più importanti enigmi matematici:

Ipotesi di Riemann. Tutti gli zeri non banali della funzione Zeta $\zeta(s)$ hanno parte reale pari ad $\frac{1}{2}$

Agli inizi del '900 venne dimostrato che, se verificata, l'Ipotesi di Riemann avrebbe introdotto un ulteriore miglioramento nella stima dell'errore presente nel Teorema dei Numeri Primi.

La soluzione di questo problema, quindi, potrebbe guidarci ad una conoscenza più precisa della funzione $\pi(x)$ e della distribuzione dei numeri primi.

[1] Il titolo originale è *"Über die Anzahl der Primzahlen unter einer gegebenen Größe"*

5. Test di Primalità e Fattorizzazione

Oltre al problema di capire come i numeri primi si distribuiscono nell'insieme dei naturali, i matematici hanno affrontato altre avvincenti sfide. Tra queste troviamo:

- *test di primalità*: riconoscere se un intero N è primo
- *fattorizzazione*: scomporre un numero N nei suoi fattori primi

Lo stesso Gauss nel suo *Disquisitiones Arithmeticae* definì questi due problemi come i più "importanti ed utili di tutta l'aritmetica". In verità dopo i primi "elementari" algoritmi proposti dai greci, ancora nel 300 a.C, non ci furono significativi progressi fino ai contributi di Fermat, nel XVII° secolo.

La tecnica proposta dai greci era di fatto elementare: dato il numero N, si procede a dividere tale numero per 2, 3, 4, 5, …, $\sqrt{N}$. Se nessuna delle divisioni dà resto 0 allora N è primo altrimenti è composito e sono noti i suoi fattori. L'algoritmo funziona, questo è certo, ma è poco efficiente e diventa proibitivo per valori di N molto grandi.

Alla base del procedimento di fattorizzazione proposto da Fermat, invece, c'è l'idea di esprimere il numero N come differenza di due quadrati, $N = x^2 - y^2$, ottenendo così i fattori $(x - y)$ e $(x + y)$.

Dopo Fermat anche Legendre e lo stesso Gauss suggerirono altre tecniche per scomporre in fattori primi un numero intero ma alla fine rimaneva il problema che gli algoritmi individuati non erano abbastanza efficienti per fattorizzare grandi numeri (con più di 10 cifre). D'altra parte, ricordiamolo, a quell'epoca i calcoli venivano eseguiti a mano su carta.

E' per tale motivo che il problema della fattorizzazione ha suscitato un rinnovato interesse solo nel XX° secolo, con l'arrivo dei calcolatori elettronici e soprattutto a partire dagli anni '70, dopo la nascita della Crittografia a Chiave pubblica. Questo perché, come vedremo in seguito, la crittografia a chiave pubblica basa la propria sicurezza sulla difficoltà nel risolvere problemi matematici particolarmente ardui e tra questi c'è anche il problema della fattorizzazione intera.

Gli algoritmi per verificare la primalità di un numero intero hanno avuto più o meno la stessa evoluzione: i contributi più importanti si sono avuti negli ultimi decenni, in seguito all'introduzione delle moderne tecniche crittografiche.

Ciò che accomuna il problema della fattorizzazione e del test di primalità è la loro natura *computazionale*; questo perché fin dai tempi degli antichi greci siamo in grado fattorizzare un numero o verificare se è primo. Il difficile stà nel riuscire ad individuare algoritmi che risolvano tali problemi in modo "computazionalmente efficiente", cioè che non richiedano troppi calcoli e che quindi possano essere applicati anche a numeri molto grandi, fornendo il risultato in tempi *ragionevoli*.

I procedimenti più diffusi per risolvere la verifica di primalità sono gli algoritmi probabilistici di Miller-Rabin e Solovay-Strassen concepiti negli anni '70. In tempi recenti, nel 2002, i tre ricercatori indiani Agrawal, Kayena e Saxena hanno proposto l'agoritmo deterministico AKS (dalle loro iniziali) che risolve il test di primalità in modo molto efficiente (con complessità polinomiale).

Per quanto riguarda il problema della fattorizzazione, invece, lo stato dell'arte è l'algoritmo General Number Field Sieve (GNFS) sviluppato verso la fine degli anni '80, particolarmente complesso ma il più veloce in assoluto.

6. Crittografia

Dopo questa veloce incursione nel mondo nei numeri primi, è giunto il momento di capire come essi vengono applicati nella moderna crittografia. Già, ma cos'è la crittografia?

La crittografia (il termine deriva dal greco *kryptòs* - nascosto e *gràphein* - scrivere) è la scienza delle scritture segrete. Per mezzo di tecniche crittografiche quindi, un messaggio viene alterato utilizzando un procedimento concordato da *mittente* e *destinatario* in modo che risulti incomprensibile ad un eventuale *avversario* che riesca ad intercettarlo. La modifica del testo in chiaro viene detta *cifratura*, mentre il procedimento inverso, che permette di ricostruire il messaggio originale, è chiamato *decifratura*.

Come già detto, mittente e destinatario devono condividere a priori una conoscenza segreta che consenta la cifratura del messaggio e la successiva decifratura. Tale conoscenza però non è il processo di modifica ma è la cosiddetta *chiave* ossia una stringa alfanumerica che costituisce un parametro della

funzione di cifratura e della funzione di decifratura. Il metodo di alterazione perciò è noto a chiunque ma ogni volta viene parametrizzato con una chiave nota solo al mittente e al destinatario. Questo concetto è conosciuto come *Principio di Kerckhoff*, dal nome del linguista-crittografo fiammingo Auguste Kerckhoff che nel 1883 postulò tale idea in un articolo intitolato "*La cryptographie militare*":

"tutti gli algoritmi devono essere pubblici, solo le chiavi sono segrete"

Gli algoritmi crittografici possono essere suddivisi in due grandi famiglie:

- **algoritmi a chiave segreta** *(simmetrici)*: i processi di cifratura e di decifratura utilizzano la stessa chiave K.
- **algoritmi a chiave pubblica** *(asimmetrici)*: la chiave di cifratura K_E è diversa dalla chiave K_D utilizzata nel processo di decifratura. Le due chiavi sono fra loro correlate.

Le tecniche simmetriche, storicamente nate per prime, sono particolarmente veloci e robuste ma richiedono che mittente e destinatario condividano in modo sicuro la chiave K. Inoltre soffrono del *Problema della distribuzione delle chiavi*: per garantire che N individui possano comunicare in modo sicuro fra loro, dovranno essere generate $\frac{N(N-1)}{2}$ chiavi (ogni persona possiede $N-1$ chiavi). Si capisce bene che con valori di N sempre più grandi la cosa diventa complicata da gestire. Esempi di algoritmi simmetrici sono: 3DES, AES, RC4.

Il concetto di crittografia a chiave pubblica è nato negli anni '70 e più precisamente è stato proposto dai ricercatori Whitfield Diffie e Martin Hellman nel loro ormai famoso articolo "*New Directions in Cryptography*" apparso nel 1976. Il principio di funzionamento è semplice: immaginiamo che Alice desideri spedire un messaggio confidenziale a Bob:

- Bob genera due chiavi: una *privata* che custodisce gelosamente ed una corrispondente chiave *pubblica* che distribuisce a tutti i suoi *pen-friend*, tra i quali c'è anche Alice.
- Alice usa la chiave pubblica di Bob per cifrare il messaggio a lui destinato.
- Bob utilizza la propria chiave privata per decifrare il messaggio ricevuto da Alice.

La cosa importante è che con la chiave pubblica si effettua la cifratura ma con la stessa NON è possibile eseguire la corrispondente decifratura: in sostanza chi possiede la chiave pubblica può solo cifrare mentre per ricostruire il messaggio è necessario utilizzare la relativa chiave privata.

In questo modo si risolve elegantemente il problema della distribuzione delle chiavi: Bob infatti deve generare una sola coppia di chiavi e può distribuire a chi vuole la propria chiave pubblica.

Le due chiavi, pubblica e privata, sono fra loro correlate ma deve essere *difficile* risalire alla seconda conoscendo la prima. Questa difficoltà è di natura matematica, o meglio, è legata ad un problema matematico particolarmente difficile da risolvere. Ad oggi i problemi matematici su cui si basa la crittografia a chiave pubblica sono:

- **Problema della fattorizzazione intera** (IFP, *Integer Factorization Problem*): dato un numero composto n ottenuto moltiplicando due grandi numeri primi p e q ($n = pq$), trovare p e q. Su questo problema si basa l'algoritmo RSA.
- **Problema del logaritmo discreto** (DLP, *Discrete Logarithm Problem*): calcolare il logaritmo di un numero intero all'interno di un gruppo finito. Su tale problema si basano gli algoritmi El-Gamal e Diffie-Hellman.
- **Problema del logaritmo discreto su curve ellittiche** (ECDLP): consiste nella risoluzione del problema del logaritmo discreto all'interno dei punti di una curva ellittica. E' alla base di tutta la crittografia su curve ellittiche.

In questa sede analizzeremo l'algoritmo RSA, ma prima di farlo dobbiamo introdurre alcuni necessari strumenti matematici.

7. Aritmetica modulare

Gli algoritmi di cifratura agiscono su insiemi di valori che sono discreti e finiti. L'aritmetica modulare consente di effettuare le normali operazioni di somma e prodotto ottenendo risultati che sono sempre all'interno di un determinato *range* di valori. Non a caso viene anche detta *aritmetica dell'orologio*: anche se i minuti "vanno continuamente avanti" rimangono sempre all'interno dell'insieme finito e discreto 0,1,2,…,59.
In sostanza, l'aritmetica modulare all'interno di un insieme finito $Z_n = \{0,1,2,\ldots,(n-1)\}$ prevede che di ogni numero se ne consideri il *residuo modulo n,* ossia:

- si svolgono le normali operazioni di somma e moltiplicazione
- si dividono i risultati per n e se ne considerano i resti (detti anche **residui**); il resto della divisione del numero a per n si indica con $\boldsymbol{a}$ **mod** $\boldsymbol{n}$.
- il numero n viene detto **modulo**.

Consideramo alcuni esempi con l'insieme finito $Z_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$:

$6 \bmod 11 = 6$ $\quad [6 = 11\cdot 0 + \mathbf{6}]$
$(8 + 7) \bmod 11 = 15 \bmod 11 = 4$ $\quad [15 = 11\cdot 1 + \mathbf{4}]$
$(6 \cdot 4) \bmod 11 = 24 \bmod 11 = 2$ $\quad [24 = 11\cdot 2 + \mathbf{2}]$

Si possono facilmente dimostrare le seguenti proprietà:

$[(a \bmod n) \pm (b \bmod n)] \bmod n = (a \pm b) \bmod n$
$[(a \bmod n)\,(b \bmod n)] \bmod n = (ab) \bmod n$

L'aritmetica modulare inoltre definisce il concetto di *congruenza*, che è paragonabile alla relazione di uguaglianza nel caso di numeri naturali (5 = 5).

Congruenza. Due numeri a e b si dicono congruenti modulo n se vale $(a \bmod n) = (b \bmod n)$ oppure, in forma equivalente, se n divide $a - b$. In tal caso si scrive:

$$\boldsymbol{a \equiv b \pmod{n}}$$

Quindi, sempre considerando l'insieme finito $Z_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$, possiamo scrivere:

$18 \equiv 7 \pmod{11}$
$12 \equiv 1 \pmod{11}$

All'interno di insiemi finiti è anche possibile definire la proprietà di inverso:
Dato un numero a, il suo *inverso moltiplicativo* in Z_n è quel numero b per il quale vale

$$\boldsymbol{ab \equiv 1 \pmod{n}}$$

A tale riguardo vale il seguente:

Teorema. Se il numero $a \in Z_n$ è tale che $\gcd(a,n) = 1$ allora a ammette inverso moltiplicativo che è unico.

Considerando Z_{11}, si ha che $n = 11$ è primo, quindi è coprimo con tutti gli elementi non nulli di Z_{11} e pertanto questi ammettono inverso moltiplicativo.
Per esempio se prendiamo $a = 4$, si trova facilmente che il suo inverso moltiplicativo è 3: infatti vale $4\cdot 3 = 12 \equiv 1 \pmod{11}$.
L'inverso moltiplicativo in Z_n di un numero a viene calcolato per mezzo dell'Algoritmo esteso di Euclide, che nella sua forma base permette di calcolare il gcd() di due numeri.

8. Funzione di Eulero φ

Molto importante nell'ambito della Teoria dei Numeri è la funzione φ (*phi*) di Eulero, così definita:

Funzione φ di Eulero. Dato l'intero n si indica con $\varphi(n)$ il numero di elementi di Z_n che sono coprimi con n; in forma sintetica

$$\phi(n) = \#\{a \in Z_n \mid \gcd(a,n) = 1\}$$

Vediamo degli esempi:

$\varphi(5) = 4$ [5 è *coprimo con tutti gli elementi non nulli di* Z_5]
$\varphi(10) = 4$ [10 *è coprimo con i numeri* 1,3,7,9]

Abbiamo già detto che se n è primo allora tutti gli elementi di Z_n sono coprimi con n stesso, pertanto vale $\varphi(n) = n - 1$. Inoltre si può facilmente dimostrare che se $n = pq$, dove p e q sono due numeri primi, allora $\varphi(n) = \varphi(pq) = \varphi(p)\,\varphi(q) = (p-1)(q-1)$.
Ad esempio:

$\varphi(21) = \varphi(3)\,\varphi(7) = (3-1)(7-1) = 12$

Come vedremo, gioca un ruolo fondamentale nel sistema di cifratura RSA il seguente:

Teorema di Eulero. Se a ed n sono coprimi, vale la seguente relazione

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Facciamo una verifica con i valori $a = 3$, $n = 10$ (che soddisfano $\gcd(a,n) = 1$):

$\varphi(10) = 4$
$3^4 = 81 \equiv 1 \pmod{10}$

Siamo ora in grado di analizzare l'algoritmo RSA.

9. Algoritmo RSA

Il sistema di cifratura RSA è stato proposto nel 1977 dai suoi tre autori Rivest, Shamir e Adleman. Oggi è senza dubbio l'algoritmo a chiave pubblica più utilizzato e il motivo di tanta popolarità risiede nella sua comprovata sicurezza. Sicurezza che si basa sul già citato problema della fattorizzazione intera (IFP): dato il numero n ottenuto moltiplicando due grandi numeri primi p e q ($n = pq$), trovare questi ultimi.
Per vedere come funziona consideriamo la situazione in cui Alice vuole spedire un messaggio confidenziale a Bob.

Generazione delle chiavi. Anzitutto, lo ricordiamo, Bob deve generare la coppia di chiavi pubblica e privata:

- seleziona due numeri primi p e q sufficientemente grandi
- calcola $n = pq$ e $\varphi(n) = (p-1)(q-1)$
- individua il numero e coprimo con $\varphi(n)$, ossia che verifichi $\gcd(e, \varphi(n))=1$
- calcola d tale che $de \equiv 1 \pmod{\varphi(n)}$

La **chiave privata** è la coppia di numeri $K_{pri} = (d,n)$ che viene conservata da Bob.
La **chiave pubblica** è la coppia di numeri $K_{pub} = (e,n)$ che viene distribuita a tutti, Alice compresa.
I valori e e d vengono detti esponente rispettivamente di cifratura e di decifratura.

Cifratura. Per cifrare il messaggio è necessario rappresentare quest'ultimo come un numero $m < n$. Alice quindi usa la chiave pubblica di Bob K_{pub} ed effettua la cifratura:

- calcola $c = m^e \bmod n$
- spedisce c a Bob

Decifratura. Ricevuto il testo cifrato c, Bob utilizza la propria chiave privata K_{pri} per ricostruire il messaggio originario m:

- calcola $m = c^d \bmod n$

In breve, durante la cifratura il messaggio m viene elevato ad e (modulo n) mentre in ricezione il testo cifrato c viene elevato a d (modulo n).

Dimostrazione

Per capire come funziona l'algoritmo RSA evidenziamo quanto segue:

- l'esponente di cifratura è stato scelto coprimo con $\varphi(n)$, in modo da ammettere inverso moltiplicativo modulo $\varphi(n)$.
- l'esponente d è proprio l'inverso moltiplicativo di e, cioè tale che $de \equiv 1 \pmod{\varphi(n)}$. Questo significa che i due esponenti soddisfano la relazione $de = k\varphi(n) + 1$, con k intero.

Vediamo ora cosa succede durante la decifratura:

$c^d \bmod n = [(m^e \bmod n)^d] \bmod n = m^{ed} \bmod n = m^{(k\varphi(n)+1)} \bmod n =$

$= [(m^{\varphi(n)})^k m] \bmod n = [(m^{\varphi(n)})^k \bmod n)\ (m \bmod n)] \bmod n = [((m^{\varphi(n)})^k \bmod n)\ m] \bmod n$ (1)

applicando il Teorema di Eulero(*), sviluppiamo il primo fattore dell'ultimo passaggio della (1) :

$(m^{\varphi(n)})^k \bmod n = [(m^{\varphi(n)} \bmod n)^k] \bmod n = 1^k \bmod n = 1$ (2)

quindi, inserendo la (2) nella (1), otteniamo proprio il messaggio originario:

$c^d \bmod n = \ldots\ldots = [((m^{\varphi(n)})^k \bmod n)\ m] \bmod n = [1 \cdot m] \bmod n = m$

(*) Al lettore più attento non sarà sfuggito che nella (2) si è applicato il Teorema di Eulero in modo improprio, perché non abbiamo fatto alcuna ipotesi sulla coprimalità fra m ed n (come richiederebbe il Teorema stesso). In realtà si può facilmente verificare che, siccome $m < n$ e quest'ultimo è uguale al prodotto di due numeri primi p e q, la dimostrazione appena vista è corretta anche per le situazioni in cui $\gcd(m,n) \neq 1$ [7, p.178].

Riepiloghiamo con un esempio:

- si considerino i primi $p = 11$ e $q = 17$, quindi $n = pq = 187$.
- calcoliamo $\varphi(187) = 160$ e i due esponenti $e = 7$, $d = 23$
- le chiavi di Bob sono: $K_{pri} = (23, 187)$ e $K_{pub} = (7, 187)$
- rappresentiamo il messaggio con il numero $m = 88$
- Alice invia il messaggio cifrato: $c = m^e \bmod n = 88^7 \bmod 187 = 11$
- Bob ricostruisce m: $c^d \bmod n = 11^{23} \bmod 187 = 88$

Sicurezza

Per un attaccante violare il sistema RSA significa recuperare il messaggio originario m a partire dal testo cifrato c. Attualmente l'unico modo conosciuto per fare questo utilizza l'esponente di decifratura d. Anche se, bisogna dirlo, non è stato dimostrato che la decifratura di c richiede necessariamente la conoscenza dell'esponente d.

In ogni caso l'attacco più ovvio consiste nel fattorizzare n nei primi p e q: così facendo è possibile calcolare $\varphi(n) = (p-1)(q-1)$ e quindi ottenere l'inverso moltiplicativo del valore e, ossia d.

Ma la fattorizzazione di n è il solo modo per "rompere" l'algoritmo RSA? Ossia è l'unico modo per recuperare l'esponente d ? In verità se si riuscisse a calcolare direttamente il valore $\varphi(n)$, senza fattorizzare n, sarebbe comunque immediato ottenere l'esponente d. Inoltre possiamo dimostrare che la conoscenza di $\varphi(n)$ permette di calcolare agevolmente i primi p e q:

- si osservi che: $\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$
- i valori p e q sono le due radici dell'equazione: $x^2 - (p+q)x + pq = 0$ (3)
- riscrivendo la (3) utilizzando $\varphi(n)$ ed n si ottiene: $x^2 - (n - \varphi(n) + 1)x + n = 0$
- di conseguenza, noti n e $\varphi(n)$ è immediato ricavare p e q.

Quindi si può dire che calcolare $\varphi(n)$ non è più facile della fattorizzazione di n, anzi, estendendo la considerazione, possiamo enunciare la seguente

Congettura RSA. Il problema di violare il sistema RSA è difficile quanto la fattorizzazione di n.

Una dimostrazione rigorosa di tale congettura non esiste ma è opinione condivisa che essa sia vera. Per realizzare un sistema RSA sicuro, quindi, il numero $n = pq$ dovrà essere abbastanza grande da rendere computazionalmente impraticabile la propria fattorizzazione. Oggi questo significa che n deve avere tra le 300 e 600 cifre decimali!

10. Conclusioni

La crittografia è una materia vasta, certamente, e insieme all'RSA vengono utilizzati numerosi altri algoritmi, sia simmetrici che asimmetrici. In ogni caso è bene sapere che quando, ad esempio, utilizziamo la nostra carta di credito per acquistare su Amazon piuttosto che per fare la spesa al supermercato noi *usiamo i numeri primi*.

Bibliografia

Un libro che spiega molto bene la Teoria dei Numeri è [2] mentre [1] descrive il legame esistente tra quest'ultima e la moderna crittografia. Nei testi [3] e [4] è possibile trovare, con numerose note storiche, un'accessibile introduzione alla funzione Zeta di Riemann e alla relativa Ipotesi. Un vero riferimento sullo studio dei numeri primi, soprattutto per gli aspetti computazionali, è [5]. I libri [6] e [7] sono due tradizionali testi di crittografia, utilizzati in corsi universitari: il primo è più attento alle applicazioni informatiche mentre il secondo cura maggiormente gli aspetti teorici degli algoritmi. Infine [8] propone una godibilissima e avvincente storia della crittografia.

[1] Leonesi S., Toffalori C., *Numeri e Crittografia*, Springer (2006)
[2] Jones G.A., Jones J.M., *Elementary Number Theory*, Springer (2005)
[3] Derbyshire J., *L'ossessione dei numeri primi*, Bollati Boringhieri (2006)
[4] Du Sautoy M., *L'enigma dei numeri primi*, BUR (2005)
[5] Crandall R., Pomerance C., *Prime numbers, a computational perspective*, Springer (2005)
[6] Stallings W., *Crittografia e Sicurezza delle Reti*, Mc Graw-Hill (2003)
[7] Paar C., Pelzl J., *Understanding Cryptography*, Springer (2010)
[8] Singh S., *Codici e segreti*, BUR (2001)

154. Moltiplicazione

di Michele T. Mazzucato

...potrà sempre da sé formar nuovi metodi e batteggiarli come gli parerà.
General trattato di numeri et misure (1556-60)
Niccolò Fontana "Tartaglia"

La moltiplicazione, insieme all'addizione, sottrazione e divisione, è una delle quattro operazioni fondamentali dell'aritmetica. I termini della moltiplicazione sono chiamati *fattori* (*moltiplicando* e *moltiplicatore*) mentre il risultato prende il nome di *prodotto*.

moltiplicando x moltiplicatore = prodotto

Le proprietà algebriche della moltiplicazione sono quella *commutativa* (scambiando l'ordine dei fattori il risultato non cambia):

$$8 \times 2 = 2 \times 8$$

associativa (se al posto di alcuni fattori si sostituisce il loro prodotto il risultato non cambia)

$$4 \times 2 \times 3 = (4 \times 2) \times 3 = 4 \times (2 \times 3)$$

dissociativa (se a uno o più fattori se ne sostituiscono altri il cui prodotto è uguale al fattore sostituito il risultato non cambia):

$$8 \times 12 = (4 \times 2) \times 12 = 8 \times (4 \times 3)$$

e *distributiva* (scomponendo un fattore si può moltiplicare l'altro fattore per ciascun termine dell'addizione o sottrazione e addizionare o sottrarre poi i prodotti parziali ottenuti):

$$14 \text{ X } 32 = 448$$
$$14 \times (24 + 8) = (14 \times 24) + (14 \times 8) = 336 + 112 = 448$$

Ogni numero moltiplicato per 1 (elemento neutro della moltiplicazione) ha come risultato il numero stesso mentre moltiplicato per 0 (elemento assorbente della moltiplicazione) ha come risultato zero.
Per indicare l'operazione della moltiplicazione si utilizzano indifferentemente i segni x, · e *. Il segno x viene accreditato a William Oughtred (1574-1660) che usò nell'opera *Clavis Mathematicae* (1631), il punto medio di moltiplicazione · venne introdotto da Gottfried Wilhelm Leibniz (1646-1716) che, in una lettera diretta a Johann Bernoulli (1667-1748) nel 1698, scrisse: *"I do not like X as a symbol for multiplication, as it is easily confounded with x..."*. Stesso segno che il prof. Dino Betti riferisce causa di confusione fra i giovani allievi argomentando: "... *che ciò sia dovuto al fatto che quando la sua maestra gli ha spiegato la moltiplicazione l'alunno non era ancora completamente lateralizzato (la lateralizzazione è la facoltà di distinguere un oggetto dipendentemente dalla sua posizione: per un bimbo di 3 anni i simboli x e + sono lo stesso simbolo e qualcuno raggiunge prima e qualche altro dopo la facoltà di distinguerli)*". Infine, il segno * introdotto da Johann Rahn (1622-1676) nell'opera *Teutsche Algebra* (1659) è oggi largamente utilizzato in informatica.
Di fatto la moltiplicazione non è altro che una addizione abbreviata. Infatti, per esempio 8 x 3 significa sommare il numero 8 tre volte ossia 8 x 3 = 8 + 8 + 8.
Dalla proprietà distributiva si deduce il metodo per eseguire la moltiplicazione di due numeri. Si scrive uno dei due numeri come somma di tante unità, decine, centinaia, etc. quante indicato dalle cifre componenti il numero in esame e si moltiplica la somma così ottenuta per l'altro numero. Per esempio:
103 x **48**

$$103 \times (4 \times 10 + 8) = (103 \times 4)x10 + 103 \times 8$$

usando lo stesso procedimento per l'altro numero si ha:

$$[(1x100 + 0x10 + 3)x4]x10 + [(1x100 + 0x10 + 3)x8] =$$

$$= 4000 + 12x10 + 8x100 + 24 = 4000 + 120 + 800 + 24 = 4944$$

Molti sono i metodi per eseguire una moltiplicazione. Vediamone alcuni esempi.

Moltiplicazione odierna

Nel Rinascimento chiamata *per bericuocolo* in Toscana (dal nome di dolcetti toscani), *per scacchiere* a Venezia, *per organetto* a Verona. Quella a noi nota e utilizzata si sviluppa nel seguente modo:

```
  103 x
   48 =
 ------
  824 +
 412  =
 ------
 4944
```

Moltiplicazione egizia (metodo dei raddoppi)

Papiro della scriba di Ahmes (1650 a.C.)

Papiro di Mosca (1850 a.C.)

Esempi se ne trovano nei due più importanti documenti matematici egizi ossia il Papiro di Ahmes o di Rhind e il Papiro di Mosca o di Goleniščev. Il primo prende il nome dallo scriba Ahmes che lo trascrisse nel 1650 a.C. circa traendolo da uno precedente risalente al 2000 a.C. circa ma anche dal nome del collezionista scozzese Alexander Henry Rhind (1833-1863) che lo acquistò nel 1858 a Luxor in Egitto. Oggi si trova al British Museum di Londra che lo acquisì nel 1863, alcuni piccoli frammenti sono conservati anche presso il Brooklyn Museum di New York. Il papiro è lungo 199,5 e largo 32 centimetri ed è scritto il lingua ieratica. Esso contiene 84 problemi matematici con le relative soluzioni e tabelle di frazioni. Il secondo, risalente al 1850 a.C. circa di autore ignoto, prende il nome dal nome dell'egittologo Vladimir Semyonovich Goleniščev (1856-1947), suo primo possessore, che lo acquistò a Tebe in Egitto nel 1893. Ceduto al governo russo nel 1911 oggi si trova presso il Museo Puškin delle belle arti di Mosca da cui l'altro nome. Il papiro è lungo 544 e largo 8 centimetri ed è scritto anch'esso in lingua ieratica e contiene 25 problemi matematici.

La moltiplicazione egizia si esegue nel seguente modo. Si formano due colonne. In quella di sinistra si fanno i raddoppi successivi partendo dall'unità fino al valore non superiore al moltiplicando 103. Nella seconda colonna si fanno i raddoppi successivi partendo dal moltiplicatore 48.

```
  1 |   48
  2 |   96
  4 |  192
  8 |  384
 16 |  768
 32 | 1536
 64 | 3072
~~128~~ |
```

poi si eseguono le sottrazioni

103-64=39
39-32= 7
7- 4= 3
3- 2= 1
1- 1= 0

64+32+4+2+1=**103**

La somma dei numeri della colonna di destra corrispondenti ai numeri sottolineati fornisce il risultato: 3072+1536+192+96+48=**4944**

Moltiplicazione russa (metodo dei raddoppi e dimezzamenti)

Sino a tempi recenti utilizzata dai contadini russi da cui il nome di moltiplicazione russa. Simile a quella egizia, essa si esegue nel modo seguente.
Si formano due colonne. In quella di sinistra si fanno i raddoppi successivi partendo dal moltiplicando 103. Nella seconda colonna si fanno i dimezzamenti successivi partendo dal moltiplicatore 48 sino al raggiungimento dell'unità. Se il numero è dispari si toglie 1 e si dimezza.

103	**48**	
206	24	
412	12	
824	6	
1648	3*	(3-1=2:2=1)
3296	1*	

La somma dei numeri della colonna di sinistra corrispondenti ai numeri dispari fornisce il risultato: 1648+3296=**4944**

Moltiplicazione indiana e araba

Metodo denominato "procedimento degli indiani" o "via degli indiani" senza cancellazione dei risultati intermedi. Un esempio di tale calcolo si trova nel *Kitāb al fusūl fi'l hisāb al hindi* (*Trattato di aritmetica indiana*) composto a Damasco nel X secolo d.C. da al Uqlīdīsī. Procedimento:

```
1)      1 0 3  moltiplicando
     4 8       moltiplicatore
```

2) si moltiplica 1x4 ottenendo 4 che si posiziona sulla colonna del 4 in una nuova riga sopra il moltiplicando e si barra il 4 del moltiplicatore:

```
4
  1 0 3
~~4~~ 8
```

3) si moltiplica 1x8 ottenendo 8 che si posiziona sulla colonna dell'1 sopra la riga del moltiplicando e si barra l'8 del moltiplicatore:

```
4 8
  1 0 3
~~4~~ ~~8~~
```

4) si barra 1 del moltiplicando e si riscrive il moltiplicatore in una riga più in basso scalando le cifre di una colonna verso destra:

4 8
~~1~~ 0 3
~~4~~ ~~8~~
4 8

5) si moltiplica 0x4 ottenendo 0 che si posiziona sulla colonna del 4 in una nuova riga sovrastante, si barra il 4 sottostante e il 4 del moltiplicatore:

4
~~4~~ ~~8~~
~~1~~ 0 3
~~4~~ ~~8~~
~~4~~ 8

6) si moltiplica 0x8 ottenendo 0 che si posiziona sulla colonna dell'8 nella riga sovrastante, si barra l'8 sottostante e l'8 del moltiplicatore:

4 8
~~4~~ ~~8~~
~~1~~ 0 3
~~4~~ ~~8~~
~~4~~ ~~8~~

7) si barra 0 del moltiplicando e si riscrive il moltiplicatore in una riga più in basso scalando le cifre di una colonna verso destra:

4 8
~~4~~ ~~8~~
~~1~~ ~~0~~ 3
~~4~~ ~~8~~
~~4~~ ~~8~~
4 8

8) si moltiplica 3x4 ottenendo 12 si scrive 2 sopra lo 0 del moltiplicando, si somma il riporto 1 all'8 che si barra, si scrive 9 sopra ad esso e si barra anche il 4 del moltiplicatore:

9
4 ~~8~~
~~4~~ ~~8~~ 2
~~1~~ ~~0~~ 3
~~4~~ ~~8~~
~~4~~ ~~8~~
~~4~~ 8

9) si moltiplica 3x8 ottenendo 24 si scrive 4 sopra al 3 del moltiplicando, si somma il riporto 2 al 2 che si barra, si scrive 4 sopra ad esso, si barra anche l'8 del moltiplicatore. Infine si barra anche il 3 del moltiplicando e i numeri restanti forniscono il risultato cercato:

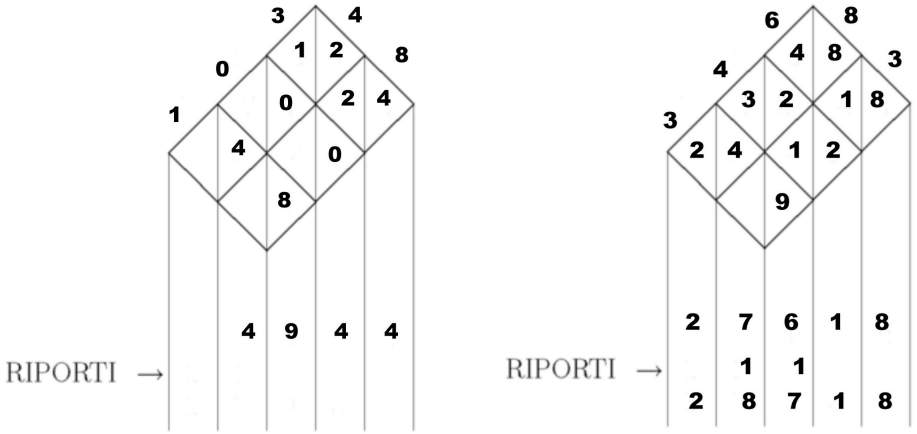
9
4 ~~8~~ **4**
~~4~~ ~~8~~ ~~2~~ **4**
~~1~~ ~~0~~ ~~3~~
~~4~~ ~~8~~
~~4~~ ~~8~~
~~4~~ ~~8~~
4 9 4 4

Moltiplicazione araba (per gelosia)

Chiamata anche moltiplicazione "per graticola" o "per reticolo". Il nome deriva dalla grata, chiamata gelosia, che veniva posta alle finestre per impedire la vista dall'esterno di ciò che succedeva all'interno della casa. Dato che il metodo presuppone l'utilizzo di un reticolo che ricorda questo tipo di grata esso stesso ha preso tale nome.

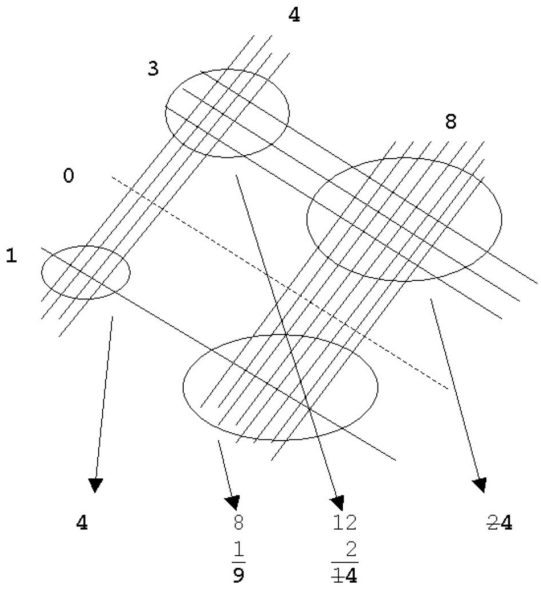
I due numeri da moltiplicare vengono posti ai lati di una tabella avente tante righe e colonne quante sono le cifre dei due fattori. Ogni quadrato viene suddiviso dalla diagonale nella cui parte superiore conterrà le decine mentre in quella inferiore le unità risultanti dalle moltiplicazioni parziali fra le cifre dei fattori. Il risultato, che viene fornito dalla somma dei numeri contenuti nelle strisce diagonali partendo da destra in basso e facendo attenzione ai riporti, è dato dalla lettura della sequenza dei numeri partendo dal lato sinistro (dall'alto verso il basso) e proseguendo sul lato inferiore (da sinistra a destra).

Effettuando una rotazione di 45 gradi del reticolo si ottiene una variazione pratica molto utile: le cifre delle strisce diagonali da sommare si trovano incolonnate verticalmente. Si vedano gli esempi in figura.



Moltiplicazione cinese (o grafica)

Si disegnano dei fasci di rette corrispondenti al valore delle cifre. Prima quelle parallele del moltiplicando 103 (una per 1, una per 0 tratteggiata e tre per 3) poi, trasversali alle prime, quelle parallele del moltiplicatore 48 (quattro per 4 e otto per 8). Il numero degli incroci fornisce il risultato. Gli incroci con la retta tratteggiata non vengono contati e bisogna fare attenzione ai riporti.



Una variante viene attribuita a Jagadguru Shankaracharya Shri Bharati Krishna Tirthaji Maharaja (1884–1960), padre riconosciuto della matematica risalente ai Veda (antichissima raccolta di testi sacri della religione induista), nonché autore di *Vedic Mathematics* pubblicato postumo nel 1965.

In quest'ultima opera si trova la moltiplicazione di un numero di due cifre per 11. Per esempio 11x32 = 352 dove
1) il 2 di 352 è dato dal 2 di 32;
2) il 5 di 352 è dato dalla somma 3+2 di 32,
3) il 3 di 352 è dato dal 3 di 32.

Il metodo vale anche per un numero di cifre maggiore di due moltiplicato per 11. Per esempio 11x458 = 5038 dove
1) l'8 di 5038 è dato dall'8 di 458;
2) il 3 di 5038 è dato dalla somma 5+8 = 1**3** (con resto 1) di 458;
3) lo 0 di 5038 è dato dalla somma di 4+5 = 9+1 (resto del punto 2) = 1**0** di 458;
4) il 5 di 5038 è dato dalla somma di 4 di 458 + 1 (resto del punto 3).

Si trova anche questa moltiplicazione equivalente alla formula (10a+b)(10c+d) = 100ac + 10(ad+bc) + bd. Per esempio 34x23 =782

3 a		4 b
|	×	|
2 c		3 d
3×2	3×3+4×2	4×3
6	17	12
1	1	
7	**8**	

Moltiplicazione per scapezzo (o per spezzato)

Per l'esecuzione si scompongono i fattori 103 e 48 della moltiplicazione nella somma di due o più addendi a piacere, per esempio

$$103 = 100 + 3 \qquad 48 = 40 + 8$$

il prodotto si ottiene applicando alla moltiplicazione

$$(100+3)\times(40+8)$$

la proprietà distributiva rispetto all'addizione.

	100	**3**
40	4000	120
8	800	24

Il prodotto è dato dalla somma di 4000+800+120+24 = 4944

Moltiplicazione per crocetta

Nota agli indiani come moltiplicazione fulminea.

103x48 = (100+3)x(40+8)

```
  40 x 100 = 4000
4000 + (3x40)= 4000 + 120 = 4120
4120 + (100x8)= 4120 + 800 = 4920
4920 + (3x8)= 4920 + 24 = 4944
```

Moltiplicazione per castelluccio

Così denominata dai fiorentini e nota anche come moltiplicazione *all'indietro*.

esempio **103x48**=

1 centinaia x8= 8 (si aggiunge 2 zeri dato che si tratta di centinaia)
1 centinaia x4= 4

0 decine x8= 0 (si aggiunge 1 zero dato che si tratta di decine)
0 decine x4= 0

3 unità x8= ~~2~~4 = 4
3 unità x4= 12+2 = 14

```
  103
x  48
 4800
  000
  144
 4944
```

esempio **346x83=**

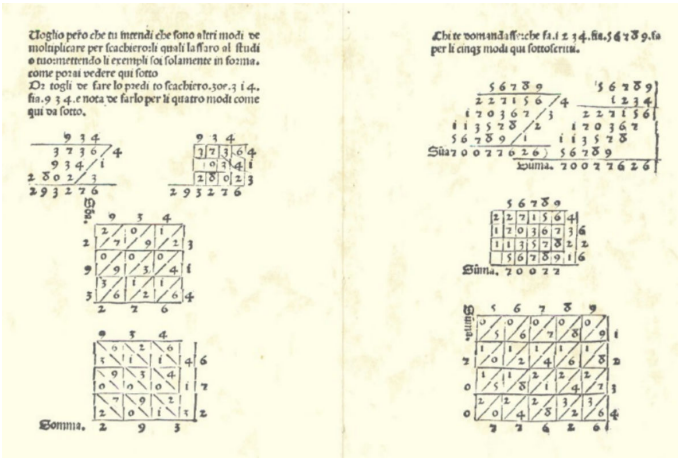
3 centinaia x 3= 9 (si aggiunge 2 zeri dato che si tratta di centinaia)
3 centinaia x 8= 24

4 decine x 3 = ~~1~~2 = 2 (si aggiunge 1 zero dato che si tratta di decine)
4 decine x 8 = 32+1 = 33

6 unità x 3 = ~~1~~8 = 8
6 unità x 8 = 48+1 = 49

```
  346
x  83
 24900
  3320
   498
 28718
```

Nuovi procedimenti e varianti degli stessi sulla moltiplicazione si trovano in vari testi fra cui si ricordano *Brahmasphutasiddhānta* (628) dell'indiano Brahmagupta nel quale descrisse quattro metodi; *Līlāvatī* (circa 1150) dell'indiano Bhāskarāchārya che descrisse un procedimento che chiamò "separazioni di posizioni"; il *Talkhīs a 'māl al hisāb* (*Esposizione sommaria di operazioni aritmetiche*) (1299) di al Marrākushī, *Miftah al Hisāb* (*Chiave dell'aritmetica*) (1427) di al Kāshī che riprende un procedimento noto già da due secoli prima e descritto nell'opera *Jami' al hisāb bi't takht wa't turāb* (*Raccolta d'aritmetica con l'aiuto di una tavoletta e della polvere*) (1265) di Nasīr ad Dīn at Tūsī; *Kashf al Mahjub min 'ilm al ghubār* (*Rilevazioni sui segreti della scienza aritmetica*) (circa 1470) di al Qalasādī; *Larte de labbacho* (Treviso, 1478) d'autore anonimo, *Arithmetica* (Venezia, 1484) di Pietro Borghi; *Summa de arithmetica, geometria, proportioni e proportionalità* (Venezia, 1494) di Frà Luca Bartolomeo de Pacioli dove espose una raccolta organica di otto metodi di moltiplicazione (*per scacchiere*, *per castelluccio*, *per colonna*, *per crocetta*, *per quadrilatero*, *per gelosia*, *per repegio* e *per scapezzo*); *General trattato di numeri et misure* (1556-60) di Niccolò Tartaglia (*per rombo*, *per triangolo*, *per coppa*, *per diamante*); *Ganitamanjarī* (1658) dell'indiano Ganesha, *Novissima prattica d'aritmetica mercantile* (Roma, 1670) di Domenico Griminelli e *Trattato aritmetico* (Venezia, 1678) di Giuseppe Maria Figatelli.



***Larte de labbacho* (Treviso, 1478) d'autore anonimo. Il primo manuale di matematica a stampa pubblicato al mondo.**

(A sn.) *La Summa de arithmetica, geometria, proportioni e proportionalità* (Venezia, 1494) di Frà Luca Bartolomeo de Pacioli. (a dx) Emissione filatelica italiana del 1994 in occasione del 500° anniversario della *Summa* (1494) di Luca Pacioli.


NOVISSIMA PRATTICA
D' ARITMETICA
MERCANTILE
Composta dal
R.D. DOMENICO GRIMINELLI
SACERDOTE DA CORREGGIO
a benefitio vniuerſale.
IN ROMA, Per il Succeſſal Mafcardi, MDCLXX.
Con licenza de' Superiori.

TRATTATO
ARITMETICO
DI
GIVSEPPE MARIA FIGATELLI
DIVISA IN DVE PARTI
In queſta ſeconda Impreſſione
Aggiontoui l'Algebra
IN VENETIA, M. DC. LXXVIII.
Preſſo Steffano Curti,
CON LICENZA DE' SVPERIORI.

(A sn.) Novissima prattica d'aritmetica mercantile (1670) di Domenico Griminelli. (A dx) Seconda edizione del Trattato aritmetico (1678) di Giuseppe Maria Figatelli (1612-1682).

Fra i molti presenti nell'opere sopra citate si riporta, come esempio, il procedimento del matematico indiano Bhāskarāchārya:

```
103x48=                          346x83=

  1 0 3     1 0 3                  3 4 6     3 4 6
    4         8                      8         3
_________ _________              _________ _________

  4 1 2     8 2 4                2 4 4 8     9 1 8
    0         0                    3 2       1 2
_________ _________              _________ _________

  4 1 2     8 2 4                2 7 6 8   1 0 3 8
_________ _________              _________ _________

      8 2 4                          1 0 3 8
    4 1 2                          2 7 6 8
_________                        _____________

  4 9 4 4                        2 8 7 1 8
```

Nella prima riga si scrive due volte il moltiplicando (perché due sono le cifre del moltiplicatore). Nella terza riga si scrivono i risultati interi delle moltiplicazioni 3x6 e 3x3 saltando quello centrale. Nella quarta riga si scrive, scalando di un posto verso sinistra, il risultato della moltiplicazione centrale precedentemente saltata. Nella sesta e settima riga si scrivono i risultati delle somme parziali da destra a sinistra scalate di un posto verso sinistra. La loro somma fornisce il risultato cercato.

Verifica della correttezza del calcolo

Per la verifica della correttezza del calcolo viene spesso utilizzata la prova del nove. Essa però non è infallibile. Se la prova è negativa sicuramente si è commesso un errore nel calcolo ma se la prova è positiva non possiamo essere certi di averlo eseguito correttamente. Leonardo da Pisa meglio conosciuto come Fibonacci (1170-1250 circa) nel *Liber Abbaci* (1202) ne forniva per la prima volta una precisa giustificazione.


(A sn) Leonardo da Pisa (Fibonacci) autore del Liber Abbaci (1202). (A dx) Emissione filatelica francese del 1962 in onore di Blaise Pascal nel suo terzo centenario della morte. Colui che fornì un criterio di divisibilità applicabile a qualsiasi numero.

Mentre Pacioli nella *Summa de arithmetica, geometria, proportioni e proportionalità* (1494) esorta per l'utilizzo della prova del sette giudicata più sicura di quella del nove. Bisognerà arrivare, tuttavia, a Blaise Pascal (1623-1662) che nel *De numeris multicibus ex sola characterum numericorum additione agnoscendis* (1650) fornirà un criterio di divisibilità applicabile a qualsiasi numero.

somma cifre primo fattore (A)	somma cifre secondo fattore (B)
somma cifre prodotto numeri (A) e (B)	somma cifre prodotto da verificare

Regola per la prova del 9.

Per esempio:

```
  103 x
   48 =
 ------
  914 +
 412  =
 ------
 5034
```

la prova del nove

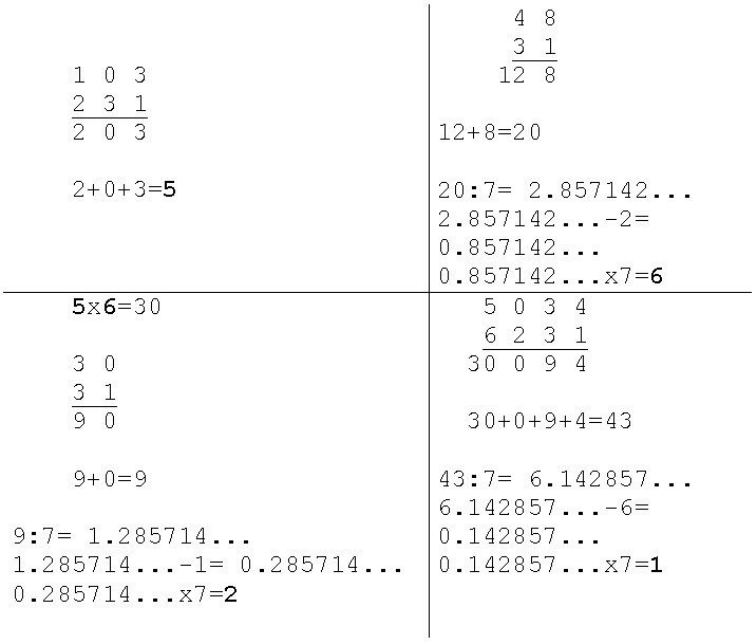
1+0+3=**4**	4+8=12 1+2=**3**
4x**3**=12 1+2=**3**	5+0+3+4=12 1+2=**3**

fornisce un esito positivo. In realtà il prodotto di 103x48 è 4944.

Per la prova del sette si considera la sequenza ciclica di numeri ...5 4 6 2 3 1 5 4 6 2 3 1 (data dai resti modulo 7 delle successive potenze di 10) e si procede:

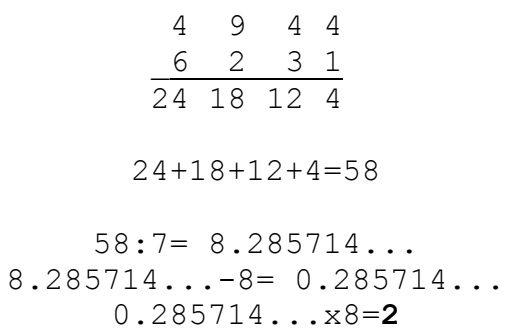
a) scrivendo su una riga le cifre del prodotto;
b) scrivendo sotto ciascuna di esse altrettanti termini della sequenza ciclica (a partire da destra);
c) moltiplicando i termini della prima riga con i corrispondenti della seconda riga;
d) sommando i prodotti ottenuti;
e) e, infine, calcolando il resto mod 7 del valore ottenuto.

Applicando all'esempio abbiamo:



Applicazione della regola del 7.

rivelando un errore nel calcolo. Inserendo il prodotto esatto 4944 si ottiene un resto concorde con quello risultante dal prodotto dei resti dei fattori 103 e 48:



Bibliografia

Bottazzini U. - Freguglia P. - Toti Rigatelli L., *Fonti per la storia della matematica*, Sansoni, Firenze, 1992
Cajori F., *A History of mathematics*, Macmillan, New York 2nd ed., 1919
Ifrah G., *Enciclopedia universale dei numeri*, Mondadori, Milano, 2008
Boyer C.B., *Storia della matematica*, Mondadori, Milano, 1990
Loria G., *Le scienze esatte nell'antica grecia,* Hoepli, Milano, 1914
Lussardi L., *Moltiplicare i numeri con la geometria*, Matematicamente.it Magazine n. 138/2010 pp. 10-14
Smith D.E., *History of Mathematics*, Ginn & Co., Boston 1923-1925 voll. I-II
http://www.vedicmathsindia.org matematica vedica

155. Frazioni e scuola dell'obbligo

Domenico Lenzi[*], Ilario Marra[**]
domenico.lenzi@unisalento.it
presidente@bachmusicacademy.it
[Dip. Mat. Uni. Salento, Lecce]

Premessa

Quello dell'insegnamento/apprendimento della matematica è un problema che negli ultimi anni è andato crescendo sempre più.
Tra gli argomenti più ostici per i nostri studenti di ogni ordine e grado ci sono le frazioni, le quali – nonostante la semplicità con cui possono essere introdotte (si pensi alle classiche porzioni di torte) – ben presto diventano incomprensibili, soprattutto per quel che riguarda le operazioni di cui vengono dotate. Ciò in parte è dovuto anche al fatto che spesso le stesse operazioni tra numeri naturali non sono state sufficientemente assimilate, almeno per quel che riguarda il significato delle loro proprietà; il che poi si riversa sui numeri frazionari, che sono una generalizzazione dei numeri naturali. Questo ci ha indotti a occuparci di frazioni nell'ambito della scuola dell'obbligo, con l'intento di smussarne alcune asperità; anche perché l'argomento è fondamentale per il successivo passaggio ai numeri reali.

1. Matematica: aspetti epistemologico-didattici

Fino a non molti anni fa il docente era visto come una figura altamente autorevole, che aveva il compito di trasmettere conoscenza ai suoi allievi; mentre il discente era considerato poco più che un recettore passivo di nozioni. Questi era semplicemente il prodotto del lavoro dell'insegnante, non essendo egli messo nelle condizioni di costruire autonomamente le sue competenze. Oggi, invece, il tradizionale modello di insegnamento si sta rivelando inadeguato. Infatti, il percorso didattico messo in atto dal docente in base a quel modello non sempre si raccorda con l'organizzazione mentale dello studente.
Secondo i recenti risultati dell'epistemologia didattica, l'acquisizione del sapere non è simile a una costruzione che si realizza mattone su mattone, ma è un reticolo dinamico (cf. [S]) dove gli apprendimenti sono acquisiti e strutturati in "mappe mentali". Perciò si tratta di ancorare opportunamente le nuove conoscenze alle precedenti, in modo tale da costruire un sapere unico sempre più ampio. Si tratta di un principio tipico del cosiddetto *costruttivismo* pedagogico, basato sul metodo del *cooperative learning*, che si fonda sulla ricerca cooperativa e quindi sulla condivisione di risorse ed esperienze. Per cui l'insegnante ha il ruolo non di informatore, ma di mediatore didattico lungo il percorso del discente verso la conoscenza; che scaturirà dal contesto concreto – in senso lato, ambientale e mentale – e dovrà avere carattere cooperativo, sociale. E, come hanno evidenziato le ricerche didattiche degli ultimi tempi, è estremamente importante il coinvolgimento diretto dello studente nella costruzione delle proprie conoscenze, che egli dovrà imparare a gestire attraverso il superamento di ostacoli didattici dovuti a nozioni acquisite in precedenza, che però spesso deb-bono essere opportunamente rielaborate, affinché se ne possa avere pieno possesso.
Tra l'altro, va tenuto presente che gli apprendimenti – non solo della matematica – sono caratterizzati da ostacoli di diversa entità, di tipo disciplinare e non, che frequentemente possono determinare degli errori. Però, mentre un tempo all'errore veniva attribuita una valenza negativa,

[*] Presidente della commissione "Alfabetizzazione" del Rotary International, Distretto 2120 (Puglia e Basilicata).
[**] Dottore in matematica e cultore di didattica della matematica.

adesso nei suoi riguardi si ha un atteggiamento più costruttivo. Infatti, ora esso non è più soltanto rivelatore del fatto che forse uno studente non è in grado di capire o non si è sufficientemente applicato, ma deve trasformarsi in una domanda per il docente, il quale deve chiedersi a cosa sia dovuto quell'errore, che quindi può essere una tappa importante nella costruzione del sapere; per questo a volte la sua comparsa può addirittura risultare provvidenziale, rivelando concetti mal compresi a cui porre rimedio.
Naturalmente, sarà importante che l'insegnante dia adeguata importanza all'uso del linguaggio, per meglio comprendere ed essere compreso. In tal modo si potrà migliorare e semplificare l'apprendimento dei bambini fin da piccoli, quando i loro stili comunicativi sono del tipo "pane al pane e vino al vino". Ciò vale soprattutto per gli apprendimenti matematici, nei quali il linguaggio ha caratteristiche di precisione che è difficile riscontrare nei linguaggi naturali, caratterizzati da ambiguità e metafore che in matematica non hanno diritto di cittadinanza, a parte i primi approcci a concetti per i quali analogie e metafore possono aiutare a comprendere. E proprio sulla precisione del linguaggio matematico l'insegnante dovrebbe far leva affinché questa caratteristica comunicativa – insieme alle altre, indubbiamente importanti ed efficaci – sia conservata dagli alunni; per evitare che essa vada persa, spingendo questi inconsapevolmente verso tipi di comunicazione approssimativi –consueti, purtroppo – che spesso sono il regno dell'ambiguità, del "così è se vi pare", del "qui lo dico e qui lo nego".

2. Il concetto di frazione

Le frazioni sono presenti nella vita e nel linguaggio di ogni giorno, basta pensare agli orologi, agli sconti, alle ricette di cucina; senza tralasciare il fatto che l'introduzione in Italia della moneta europea ci ha portato a dover fare i conti anche con i centesimi di euro. Il famoso quartino (di un litro vino) o un quarto di litro di latte – senza tralasciare una canzone di Domenico Modugno che cantava che *il peso sulla luna è la metà della metà* (del peso sulla terra; *n. d. r.*) – sono un formidabile punto di partenza per avviare il bambino al concetto di frazione.
Nel linguaggio comune, la parola "frazione" indica generalmente una porzione di qualcosa. In analogia, nel linguaggio matematico il termine "frazione" scaturisce dai diversi modi di suddividere in parti uguali una "cosa" considerata come unità, come un tutt'uno (per il quale in seguito useremo spesso il termine *grandezza*), che potrebbe essere il liquido contenuto in un recipiente, o la classica torta (che in sede didattica potrà essere sostituita da fogli A_4 per fotocopiatrici, facilmente reperibili) o altro.
Quale che sia il numero delle parti uguali, ognuna di esse è detta *unità frazionaria* (della *grandezza* iniziale). Inoltre, il numero di parti in cui è stata suddivisa quella grandezza si chiama *denominatore*, in quanto denomina, dà un nome al tipo di suddivisione; mentre il numero di parti prese in considerazione – proprio per tale ragione – è chiamato *numeratore*. Noi a volte li designeremo come i *termini* di una frazione.
Usualmente, il numeratore a e il denominatore b si collocano rispettivamente al di sopra e al di sotto di una sbarretta, detta *linea di frazione*: $\frac{a}{b}$ (ma talora si scrive anche a/b). Il simbolo che ne risulta, ma più propriamente il processo descritto – che quel simbolo rappresenta – viene detto *frazione*. Se il numeratore è 1, si parla di *frazione unitaria*.

Perciò – tanto per fare un esempio concreto – il procedimento svolto dalla frazione $\frac{3}{4}$ nei riguardi di una torta fa di $\frac{3}{4}$ una sorta di *operatore* costituito da due processi elementari (si veda fig. 1):

a) suddividere la torta in 4 parti uguali;

b) prendere tre di quelle parti; il che corrisponde a riprodurre una parte 3 volte.

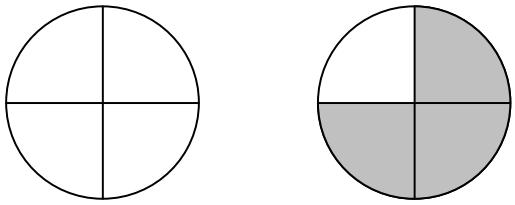


fig. 1

Naturalmente, va subito detto che, anche se dalla nostra torta abbiamo ricavato quattro parti, niente ci vieta di pensare di considerarne anche cinque, sei o più ($\frac{5}{4}$, $\frac{6}{4}$, …); così come, in presenza di quattro caramelle, niente ci vieta di pensarne – o magari di desiderarne – più di quattro. È chiaro che per realizzare ciò avremo bisogno di un numero opportuno di torte uguali tra loro, da suddividere ciascuna in quattro parti uguali.
Se il numeratore è maggiore del denominatore, generalmente si parla di *frazione impropria*. Inoltre, se il numeratore è un multiplo del denominatore, allora si parla di *frazione apparente*, dal momento che in tal caso – come si capirà agevolmente – la frazione corrisponde a un numero intero.
Facciamo presente che prendere tre quarti di una torta è come prenderne un quarto in ciascuna di tre torte uguali tra loro (si veda fig. 2 e la si confronti con la parte destra di fig. 1).

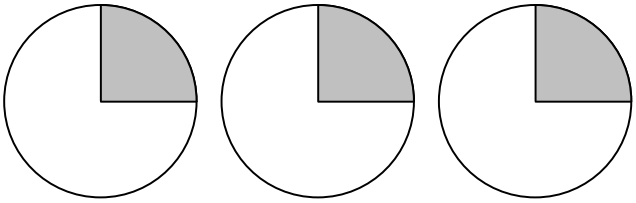


fig. 2

Perciò i $\frac{3}{4}$ di una torta corrispondono quantitativamente al conseguimento di un altro tipo di obiettivo, che non sempre è legato al *frazionare*, allo spezzettare, bensì al distribuire. Il che a volte può comportare solo alla fine il fatto di dover spezzettare. In tal caso si realizza un'alternativa alla divisione con resto.
In breve, se abbiamo tre torte da distribuire in parti uguali fra quattro bambini, come faremo? Proviamo a chiederlo ad alunni di terza elementare che abbiano già svolto il percorso illustrato precedentemente. Naturalmente, quelle tre torte dovremo fargliele vedere – magari sostituendole con dei fogli A_4 – affinché essi si possano meglio immedesimare nel *problema*.

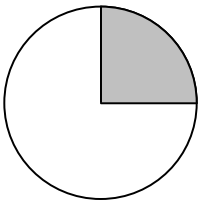


fig. 3

Inizialmente si partirà da una sola torta. In tal caso non c'è dubbio che tutti saranno convinti che ognuno di quei quattro bambini verrà ad avere $\frac{1}{4}$ di torta (si veda fig. 3).

Perciò, se le torte diventano tre (come in fig. 2), basterà svolgere la stessa procedura tre volte, e ognuno dei quattro bambini avrà tre *fette*. Quindi è come se ognuno dei quattro bambini venisse ad avere, in termini quantitativi, i $\frac{3}{4}$ di una torta.

Ciò fa capire che i due processi elementari che caratterizzano una frazione possono essere scambiati tra di loro. Vale a dire: nel caso descritto una torta prima si suppone di riprodurla 3 volte. Dopodiché del complesso di torte ottenuto viene considerata la quarta parte, procedendo alla suddivisione di ciascuna torta in quattro parti uguali.
È bene notare che tre torte suddivise ciascuna in quattro parti uguali corrispondono a un totale di 4x3 parti, ciascuna di *un quarto* (si veda fig. 4).

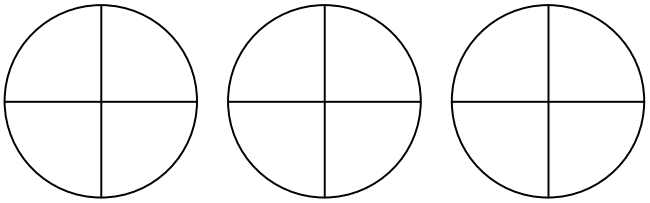


fig. 4

Analogamente, se le torte sono cinque, ognuno dei quattro bambini avrà $\frac{1}{4}$ di torta da ognuna delle cinque torte; cioè, i $\frac{5}{4}$ di una torta. Il che sarà come dare prima a ciascuno dei quattro bambini una torta intera, che corrisponde a quattro fette; poi si distribuirà a ciascuno anche un quarto della torta residua, la quale rappresenta l'intervento di $\frac{1}{4}$ su quello che prima per i bambini era il *resto* indiviso.

3. Sul confronto tra frazioni

È ben nota la relazione d'equivalenza tra frazioni, che si stabilisce sin dalla scuola primaria. In termini semplici e concreti, si può dire che due frazioni $\frac{a}{b}$ e $\frac{c}{d}$ sono equivalenti quando esse come operatori – nel senso precisato nel paragrafo 2 – sono in grado di produrre lo stesso risultato su di una stessa *grandezza* iniziale.

In tal caso si dovrebbe scrivere $\frac{a}{b} \equiv \frac{c}{d}$; ma, con un piccolo abuso di notazione, giustificato dal fatto che $\frac{a}{b}$ e $\frac{c}{d}$ hanno lo stesso "comportamento", si preferisce scrivere $\frac{a}{b} = \frac{c}{d}$, e quasi sempre si dice che $\frac{a}{b}$ e $\frac{c}{d}$ sono uguali.

Ovviamente, se due frazioni hanno lo stesso denominatore, allora per essere uguali – o meglio, equivalenti – esse debbono avere anche lo stesso numeratore; altrimenti, quella che ha numeratore maggiore determina una quantità maggiore. D'altro canto, se esse hanno lo stesso numeratore, allora per determinare una stessa quantità frazionaria debbono avere anche lo stesso denominatore; altrimenti, quella che ha denominatore minore determina una quantità maggiore.
Infatti, rispetto a una fissata grandezza, denominatore minore significa porzioni più grandi ([1]).

([1]) In concreto, con un denominatore minore, è come se una torta fosse da suddividere tra un minor numero di bambini, onde le varie porzioni saranno più grandi. Su questo aspetto è bene che l'insegnante si soffermi in modo adeguato.

In generale, moltiplicando o dividendo entrambi i termini di una frazione $\frac{a}{b}$ per uno stesso numero, si ottiene una frazione $\frac{c}{d}$ equivalente a quella di partenza. Ma come si può far prendere coscienza di ciò a un alunno? Cercheremo di farglielo intravvedere.
A tal fine sarà il caso di usare dei fogli di carta A4 (ma noi in seguito parleremo semplicemente di *fogli*). Ebbene, se abbiamo tre fogli da distribuire a due bambini, a ognuno toccheranno $\frac{3}{2}$ di foglio ("tre mezzi fogli"). Però, se i bambini raddoppiano, è chiaro che per continuare a dare a tutti quella stessa quantità, si dovranno raddoppiare anche i fogli da distribuire: altri due bambini, altri tre fogli! E se i bambini triplicano bisognerà triplicare anche i tre fogli di carta.
Il problema di decidere se due frazioni sono equivalenti (uguali) può essere facilitato parlando di frazioni ridotte [ai minimi termini ([2])]. Infatti questa riduzione si svolge dividendo numeratore e denominatore di una frazione per il massimo numero per cui entrambi possono essere divisi [che, come è noto, è il massimo comun divisore tra quei termini]. Perciò, per quanto è stato detto in precedenza, la frazione che si ottiene con la riduzione ai minimi termini è equivalente a quella di partenza.
Ciò giustifica il nome di "frazione apparente" dato a ogni frazione che abbia un numeratore che è multiplo del denominatore. Infatti essa è equivalente a una frazione avente 1 per denominatore, che perciò si può identificare con un numero naturale. In particolare: $\frac{8}{2} = \frac{4}{1}$; e $\frac{4}{1}$ si identifica con 4.

Osservazione 1. In un secondo momento l'allievo sarà indotto dall'insegnante ad accettare il fatto che due frazioni ridotte ai minimi termini che differiscano in entrambi i termini non possono essere equivalenti. In una scuola secondaria ciò può anche essere oggetto di un tentativo di dimostrazione, utilizzando in parte ciò che stiamo per dire.
Si fa presente che per decidere se due frazioni sono equivalenti c'è un criterio facile da verificare. Infatti, date due frazioni $\frac{a}{b}$ e $\frac{c}{d}$, basta moltiplicare entrambi i termini di una per il denominatore dell'altra. Così avremo le due nuove frazioni $\frac{ad}{bd}$ e $\frac{bc}{bd}$; onde queste ultime determinano rispettivamente le stesse quantità di $\frac{a}{b}$ e $\frac{c}{d}$. Inoltre, poiché $\frac{ad}{bd}$ e $\frac{bc}{bd}$ hanno lo stesso denominatore, queste quantità – come si è detto – coincidono se e solo se $\frac{ad}{bd}$ e $\frac{bc}{bd}$ hanno lo stesso numeratore; cioè, $ad = bc$.

Invece, se $ad > bc$, (rispettivamente $ad < bc$) allora già sappiamo che $\frac{ad}{bd}$ determina una quantità maggiore (rispettivamente minore) di $\frac{bc}{bd}$; quindi anche $\frac{a}{b}$ determina una quantità maggiore (rispettivamente minore) di $\frac{c}{d}$.
In definitiva, due frazioni sono tra loro equivalenti se e solo se il prodotto del numeratore della prima per il denominatore della seconda coincide col prodotto del numeratore della seconda per il denominatore della prima. Altrimenti, la frazione che realizza una quantità maggiore è quella il cui numeratore è presente nel più grande dei due prodotti ottenuti.

([2]) Ricordiamo che una frazione si dice ridotta ai minimi termini quando essa ha numeratore e denominatore che non possono essere divisi per uno stesso numero (cioè, sono primi tra loro).

4. Alcuni errori nello studio delle frazioni

Secondo alcuni studiosi un'estensione del concetto di numero naturale sarebbe più facile da accettare attraverso le *scritture decimali*, in cui i ragazzi colgono spontaneamente il significato di numero, considerando quelle decimali come rappresentazioni di numeri, ma "con in più la virgola". Per far chiarezza l'insegnante – dopo aver introdotto le frazioni – dovrebbe parlare al più presto di sistema metrico decimale, in cui la rappresentazione di una grandezza (dopo che sia stata fissata un'unità di misura) esprime il fatto che ogni cifra situata dopo la virgola rappresenta il numeratore di una particolare frazione. Quel numeratore è più piccolo di 10 proprio in conseguenza del suo significato in termini decimali (si veda [L_1]); mentre il denominatore è una potenza di 10, il cui esponente è dato dalla posizione che la cifra considerata ha nella rappresentazione decimale: esponente 1 se la cifra si trova al primo posto dopo la virgola (onde il denominatore indica la decima parte dell'unità di misura), esponente 2 se la cifra si trova al secondo posto (e il denominatore indica la centesima parte dell'unità di misura), e così via. Ragion per cui un numero decimale rappresenta la somma di un numero naturale e di una o più frazioni decimali.

Quanto detto, oltre a far chiarezza sui numeri decimali, dovrebbe evitare la comparsa di errori legati al confronto tra questi. Come $3{,}4 < 3{,}39$; che è dovuto al fatto che $4 < 39$ ([3]). Il che evidenzia la scarsa comprensione del valore posizionale delle cifre nella scrittura decimale; con buona pace di coloro che contestano l'uso dello strumento principe ai fini di questa comprensione: l'*abaco* (si veda ancora [L_1]).

Quel tipo di errore è diffuso più di quanto non si pensi ed è stato ripetutamente evidenziato dagli insegnanti. Esso è dovuto anche al fatto che non sempre appare naturale scrivere 3,4 come 3,40. Ciò a causa di una regola acquisita in modo acritico (abaco, dov'eri?), secondo cui aggiungere 0 in fondo a destra alla rappresentazione di un numero, vuol dire moltiplicarlo per 10; però dimenticando che ciò vale per i numeri naturali in quanto l'aggiunzione dello 0 altera la posizione delle cifre preesistenti, spostandole di un posto verso sinistra. Invece per i numeri decimali non cambia niente in quanto la posizione deve essere valutata rispetto alla virgola, che per i numeri naturali deve essere considerata sottintesa alla fine della scrittura, insieme a un numero arbitrario di *zeri*. Perciò l'uso dello 0 in una scrittura decimale segnala che nella casella decimale interessata "non c'è niente": il segno 0 al secondo posto dopo la virgola, dice semplicemente che in quella posizione è rappresentata la frazione *zero centesimi*; onde esso non fa altro che sostituire un'asticella vuota dell'abaco.

Il precedente errore spesso viaggia di pari passo con quello che fa cercare il "successivo" di un numero decimale (come se questo potesse esistere!); col risultato che il successivo di 0,6 è visto in 0,7; interpretando in maniera erronea il fatto che, nell'insieme dei numeri naturali, 7 è il successivo di 6. Un tale inconveniente a sua volta fa il paio con quello secondo cui $\frac{4}{5}$ è il successivo di $\frac{3}{5}$; trascurando il fatto che $\frac{4}{5} = 0{,}8$ e $\frac{3}{5} = 0{,}6$. Errori analoghi, ma più gravi, li si ritrova anche quando si tratta di ordinare frazioni che hanno denominatori diversi.

Per esempio, è frequente che si ponga $\frac{2}{3} < \frac{4}{9}$, dato che $2 < 4$. Il che è un po' come se si dicesse, in termini di peso, che due elefanti sono meno che quattro formiche.

Qui siamo di fronte a errori che Brousseau (si veda [Br]) chiama "epistemologici", dovuti a conoscenze precedenti acquisite in maniera non organica, legate a contesti numerici particolari; perciò queste non possono essere estese automaticamente a contesti più ampi.

Il fatto di considerare una frazione come una coppia di numeri può portare a errori anche nel momento in cui devono essere affrontati problemi di operazioni tra frazioni. Per esempio, a

([3]) Come è stato evidenziato in [F], errori di questo tipo li si ritrova anche in studenti delle scuole superiori. Per quel che riguarda gli errori riguardanti le frazioni si può consultare anche [B].

$n(\frac{a}{b})$ – dove n, a e b sono numeri naturali, con $b \neq 0$ – si dà come risultato $\frac{na}{nb}$; dimenticando che $n(\frac{a}{b})$ esprime la somma di n addendi eguali alla frazione $\frac{a}{b}$; fatti salvi i casi particolari per cui – in analogia con la moltiplicazione tra numeri naturali – torna utile porre: $0\left(\frac{a}{b}\right)=\frac{0a}{b}=0$ e $1\left(\frac{a}{b}\right)=\frac{a}{b}$. Perciò in ogni caso risulta: $n\left(\frac{a}{b}\right)=\frac{na}{b}$.

Osservazione 2. Fra i tanti errori, la letteratura in didattica della matematica segnala anche quelli relativi alla gestione dell'equivalenza tra frazioni. Per esempio, si considerino i quesiti legati alle scritture riportate qui di seguito:

$$\frac{1}{3}=\frac{2}{?} \qquad \frac{2}{7}=\frac{?}{14} \qquad \frac{2}{7}=\frac{?}{14}=\frac{10}{?} \qquad \frac{4}{12}=\frac{1}{?}$$

Nei primi due casi (cfr. [P]) sono frequenti le risposte esatte, invece meno del 30% risponde correttamente al terzo quesito. Inoltre, per molti alunni è più facile passare da frazioni con numeratore e denominatore più piccoli a quelle equivalenti con numeratore e denominatore più grandi; piuttosto che viceversa, come nel quarto caso. Ciò forse è dovuto al fatto che, se non è opportunamente introdotta, la divisione tra numeri naturali risulta più complicata della moltiplicazione.

5. Operazioni tra frazioni

Quanto è stato illustrato precedentemente giustifica il modo di addizionare e di moltiplicare due frazioni, o meglio, due *numeri frazionari*; designando con tale terminologia le classi rispetto all'equivalenza presentata nel paragrafo precedente.

Osservazione 3. A dire il vero, più che di equivalenza bisognerebbe parlare di *congruenza*, in analogia con la terminologia che lo stesso David Hilbert diffuse nel caso dei segmenti (si veda [H], pag. 12), estendendola poi ad altre figure geometriche. Però egli, in alternativa, usava anche il termine "uguaglianza" ([4]).

Generalmente, il termine "congruenza" viene adoperato per equivalenze tra oggetti di un certo insieme in cui siano definite delle operazioni tali che, operando su due dati oggetti oppure tra altri due oggetti rispettivamente equivalenti ai primi, si abbiano due risultati che sono tra loro equivalenti (si veda [H], pag. 13).
Ad esempio, si pensi alla somma di due segmenti. Ebbene se si sommano due altri segmenti che abbiano rispettivamente la stessa lunghezza dei primi due, è chiaro che il nuovo segmento ha la stessa lunghezza del segmento ottenuto sommando i primi due. Ebbene, come vedremo, qualcosa di simile avviene sia per la somma che per la moltiplicazione tra frazioni.

Il problema dell'addizione tra due frazioni nasce dalla seguente situazione:

> si mettano insieme le due quote determinate da due frazioni applicate a una certa grandezza che indichiamo con T [iniziale di *Torta*]. Ebbene, ci si chiede se ci sia una frazione che da sola sia in grado di produrre la stessa quota prodotta complessivamente dalle due frazioni di partenza.

([4]) Che usualmente si fa corrispondere al fatto che due segmenti abbiano la stessa lunghezza.

È chiaro che se quelle frazioni hanno lo stesso denominatore, non c'è alcun problema. Infatti, è ovvio che $\frac{3}{4}$ di torta insieme a $\frac{5}{4}$ di torta danno complessivamente 3+5 quarti di torta; così come tre caramelle più cinque caramelle danno complessivamente 3+5 caramelle. In definitiva, si ha:

$$\frac{a}{b}+\frac{c}{b}=\frac{a+c}{b}.$$

Perciò, se le due frazioni hanno denominatori diversi, basterà trasformarle in due frazioni che abbiano lo stesso denominatore e che siano rispettivamente equivalenti a quelle di partenza (cioè, ricordiamolo, producano lo stesso effetto di quelle). A tal fine si potrà usare il criterio di riduzione allo stesso denominatore usato nel paragrafo precedente ([5]), onde avremo:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad}{bd}+\frac{bc}{bd}=\frac{ad+bc}{bd}.$$

Ma c'è anche un altro tipo di problema. Precisamente:

> Data una certa grandezza T, facciamo agire su di essa la frazione $\frac{c}{d}$, il cui risultato è la grandezza che indichiamo con $\frac{c}{d}T$. Quindi sulla grandezza $\frac{c}{d}T$ facciamo agire la frazione $\frac{a}{b}$, il cui risultato è la grandezza che indichiamo con $\frac{a}{b}\left(\frac{c}{d}T\right)$. Ci si chiede se ci sia una frazione che da sola sia in grado di produrre $\frac{a}{b}\left(\frac{c}{d}T\right)$.

Anche qui la risposta è positiva e conduce, come vedremo, alla ben nota moltiplicazione tra frazioni. Perciò quella frazione la indichiamo così:

$$\frac{a}{b}\cdot\frac{c}{d}.$$

Nota Bene. Facciamo presente che ricondurre $\frac{a}{b}\cdot\frac{c}{d}$ ad $\frac{a}{b}\left(\frac{c}{d}T\right)$, corrisponde ad una proprietà dei numeri naturali. Ad esempio, $3\cdot 4$ torte (in breve, $3\cdot 4\,T$) si ottengono da 4 torte ripetute 3 volte: $3(4\,T)$; per un totale di 12 torte.

Procedendo per semplicità in un caso concreto, $\frac{2}{3}\left(\frac{3}{5}T\right)$ significa che prima di T si considerano i $\frac{3}{5}$, cioè $\frac{3}{5}\,T$; dopodiché di $\frac{3}{5}\,T$, si considerano i $\frac{2}{3}$.

Però, suddividere $\frac{3}{5}\,T$ in tre parti, significa prendere una sola delle tre porzioni espresse da $\frac{3}{5}\,T$; cioè $\frac{1}{5}\,T$. Poi $\frac{1}{5}\,T$ va considerato 2 volte, onde si ottiene $\frac{2}{5}\,T$. In definitiva, si ha:

([5]) O anche quello di riduzione al minimo comun denominatore, che però richiede il calcolo del minimo comune multiplo tra i due denominatori di partenza.

$$\frac{2}{3}\left(\frac{3}{5}T\right)=\frac{2}{5}T\,.$$

Perciò è naturale porre:

$$\frac{2}{3}\cdot\frac{3}{5}\;=\;\frac{2}{5}\,.$$

È chiaro che questo tipo di discorso si può estendere a qualsiasi coppia di frazioni $\frac{a}{b}$ e $\frac{c}{d}$ tali che $b = c$. Quindi si pone:

$$(*)\quad \frac{a}{b}\cdot\frac{b}{d}=\frac{a}{d}\,.$$

Di conseguenza nel caso generale, date le frazioni $\frac{a}{b}$ e $\frac{c}{d}$, è chiaro come procedere nel caso in cui sia $b \neq c$. Infatti, basta trasformare ciascuna delle due frazioni $\frac{a}{b}$ e $\frac{c}{d}$ in una frazione a essa equivalente, in modo che ci si possa riportare alla situazione di cui alla (*). A tal fine, basta moltiplicare i termini della prima frazione per c e quelli della seconda per b. In questo caso, $\frac{a}{b}$ e $\frac{c}{d}$ si trasformano rispettivamente così:

$$\frac{ac}{bc}\,,\;\frac{bc}{bd}\,.$$

Perciò, per il significato di equivalenza tra frazioni, risulta:

$$(**)\quad \frac{a}{b}\left(\frac{c}{d}T\right)=\frac{ac}{bc}\left(\frac{bc}{bd}T\right)\,.$$

Poiché per la (*) risulta $\frac{ac}{bc}\cdot\frac{bc}{bd}\;=\;\frac{ac}{bd}$, allora grazie alla (**) è naturale porre:

$$\frac{a}{b}\cdot\frac{c}{d}\;=\;\frac{ac}{bd}\,.$$

Sottolineiamo come l'addizione e la moltiplicazione scaturiscano da due problemi di diverso tipo, perciò bisognerebbe far notare agli allievi che non c'è alcuna giustificazione perché per le due operazioni si debba procedere in maniera analoga. In definitiva, non c'è ragione perché per addizionare $\frac{a}{b}$ e $\frac{c}{d}$ si consideri la frazione $\frac{a+c}{b+d}$; anche se $\frac{a}{b}\cdot\frac{c}{d}\;=\;\frac{ac}{bd}$.
Per quel che riguarda la sottrazione e la divisione tra frazioni, esse possono essere riguardate come operazioni inverse rispettivamente dell'addizione e della moltiplicazione; così come già avviene nel caso particolare dei numeri interi.
Concludiamo facendo presente che il concetto di numero razionale scaturisce da quello di frazione. Infatti la parola "razionale" deriva da "razione", che significa porzione, parte. E come abbiamo visto, lo studio delle frazioni è un modo per parlare di certi tipi di "razioni". Ebbene, per *numero razionale* si intende una data frazione insieme a tutte quelle a essa equivalenti.
A volte un numero razionale lo si identifica con l'azione che una frazione e tutte quelle a essa equivalenti svolgono su di una data grandezza. Il che rappresenta la "faccia concreta" del concetto di numero razionale

Questo articolo è frutto della rielaborazione di alcune parti sia di [L], sia della tesi di laurea triennale in matematica di Ilario Marra (Università del Salento, a. a. 2009-10; relatore D. Lenzi).

Bibliografia

[B] C. Bonotto, "Origini concettuali di errori che si riscontrano nel confrontare numeri decimali e frazioni", in *L'insegnamento della matematica e delle scienze integrate*, Vol. 16, n.1 (1993).

[Br] G. Brousseau, "Ingegneria didattica ed epistemologia della matematica", in *L'insegnamento della matematica e delle scienze integrate*, Bologna, Pitagora Editrice (2008).

[C] L. Campaniolo, "Didattica delle frazioni", Università di Palermo (2007).

http://www.matematicamente.it/didattica/percorsi_didattici/didattica_delle_frazioni_20090407 5245/

[F] A. Foschi, "Rapporto sull'apprendimento/insegnamento dei numeri decimali e del loro ordine", in *L'insegnamento della matematica e delle scienze integrate*, Bologna, Pitagora Editrice, Vol. 33B, N.5 (2010).

[H] D. Hilbert, *Fondamenti della Geometria* (con introduzione di Carlo Felice Manara) , Milano, Feltrinelli, (1970). Traduzione di *Grundlagen der Geometrie*, Stuttgart, B. G. Teubner (1968), decima edi-zione; prima edizione 1899.

[L] D. Lenzi, "Povera e nuda vai, Matematica!", in *Matematicamente.it Magazine*, N. 3 (2007).

[L1] D. Lenzi, "Un uso appropriato e coordinato dei Blocchi Aritmetici Multibase e dell'Abaco". http://www.educationduepuntozero.it/speciali/pdf/lenzi4_all.pdf

[M] G. Melzi, "Matematica e comunicazione sociale", in *Periodico di matematiche*, 1-2, 1978.

[P] M. I. Fandiño Pinilla, *Le frazioni aspetti concettuali e didattici,* Pitagora editrice (2005).

[S] C. W. Schminke, "Recupero e sostegno in matematica – Frazioni e Numeri Decimali", Ed. Erickson (1993)

Fractions of Me by Arys Chien

http://www.flickr.com/photos/aryschien/3433759375/

Matematicamente.it
• NUMERO 15 – MAGGIO 2011 •

156. Sul reticolo della dama

Bruno Sanchini
brunosanchini@yahoo.it

Abstract

The "family of segments":

$$\frac{y-h}{\tan\theta_0}=\begin{cases}\pm\left(|x+h|-R\cos^n\theta_0 k\right); & k^2\le\left(\frac{x+h}{R\cos^n\theta_0}\right)^2\le(1+k)^2;\quad k=1,3,5,...\\ \pm\left(R\cos^n\theta_0+R\cos^n\theta_0 k-|x+h|\right); & k^2\le\left(\frac{x+h}{R\cos^n\theta_0}\right)^2\le(1+k)^2;\quad k=0,2,4,...\end{cases}$$

$R>0; n=1,2,3,...; 0°<\theta_0<90°; h=0,\pm R\cos^n\theta_0,\pm 2R\cos^n\theta_0,...$ is used in order to find the checkers reticle.

Introduzione

Tanto per restare nel campo dello studio di grandi famiglie di segmenti, obiettivo del presente articolo è quello di trovare l'equazione del reticolo della dama ovvero l'equazione del contorno dei 64 quadrati che compongono la dama. Sarà grazie all'aiuto della rete intrecciata a maglia rombica che si potrà ottenere tale risultato.

Infatti nella prima parte del lavoro verranno identificate le equazioni di particolari famiglie della rete infinita a maglia quadrata, chiamate porzioni, mentre nella seconda parte verrà ricavata l'equazione del reticolo cercato.

Ci si riferisce in questa analisi al reticolo della dama (8 x 8 quadrati) anche se nulla ci impedirebbe di trovare, per estensione, l'equazione di un reticolo più grande di $l\times l$ quadrati con $l=9,10,..$

Il concetto basilare del presente studio è l'equazione della rete intrecciata a maglia rombica

$$\frac{y-h}{\tan\theta_0}=\begin{cases}\pm\left(|x+h|-R\cos^n\theta_0 k\right); & k^2\le\left(\frac{x+h}{R\cos^n\theta_0}\right)^2\le(1+k)^2;\quad k=1,3,5,...\\ \pm\left(R\cos^n\theta_0+R\cos^n\theta_0 k-|x+h|\right); & k^2\le\left(\frac{x+h}{R\cos^n\theta_0}\right)^2\le(1+k)^2;\quad k=0,2,4,...\end{cases}$$

$R>0; n=1,2,3,...; 0°<\theta_0<90°; h=0,\pm R\cos^n\theta_0,\pm 2R\cos^n\theta_0,...$

L'articolo è organizzato in cinque sezioni: all'introduzione segue un approfondimento sui concetti di base utili a comprendere il contributo dei risultati seguenti La terza sezione definisce alcune particolari famiglie della rete che vengono collegate nella quarta sezione in cui di definisce il reticolo della dama. Alcuni complementi sono analizzati nella quinta e ultima sezione.

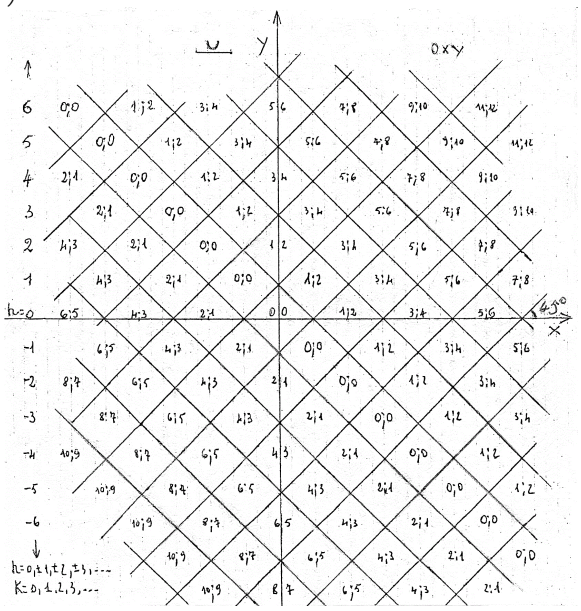
Nozioni preliminari

Se si considera l'equazione della rete intrecciata a maglia rombica nel caso particolare di $\theta_0 = 45°$ (che corrisponde quindi a $\tan 45° = 1$) e $R\cos^n \theta_0 = 1$ si otterrà la seguente funzione

$$y - h = \begin{cases} \pm\left(|x+h| - k\right); & k^2 \le (x+h)^2 \le (1+k)^2; \quad k = 1,3,5,... \\ \pm\left(1+k-|x+h|\right); & k^2 \le (x+h)^2 \le (1+k)^2; \quad k = 0,2,4,... \end{cases}$$

$h = 0, \pm 1, \pm 2, ...$ il cui diagramma è una rete infinita a maglia quadrata (si tratta di due fasci di rette parallele e perpendicolari fra loro).

Di seguito la figura su cui vengono scritti i valori di h e k (h in verticale e k all'interno di ogni metà quadrato o coppia di segmenti).



La motivazione del posizionamento dei due parametri h e k ha il significato che per ogni coppia di valori h e k presi nello stesso rigo, l'equazione che ne corrisponderà avrà come diagramma due coppie di segmenti, ognuna contrassegnata dal valore di k.

Di conseguenza, la conoscenza dei valori di h e k letti sulla rete (su parte di essa) ci consentirà di poter studiare tale parte della rete e in particolare di ricercarne la sua equazione. Viceversa, dati i valori di h e k, per poter identificare quella parte della rete che l'equazione rappresenta (vale a dire la sua rappresentazione geometrica) sarà possibile semplicemente operare sul diagramma della rete e non esclusivamente sull'equazione. Alcuni esempi illustrativi della metodologia saranno utili al fine di comprendere come si procede per trovare i valori di k che vengono poi trascritti nella rete. Vediamoli in dettaglio:

1) $h = -6 \quad e \quad 2 \le x \le 3 \quad \Rightarrow \quad -4 \le x - 6 \le -3 \quad ; \quad k = 3$

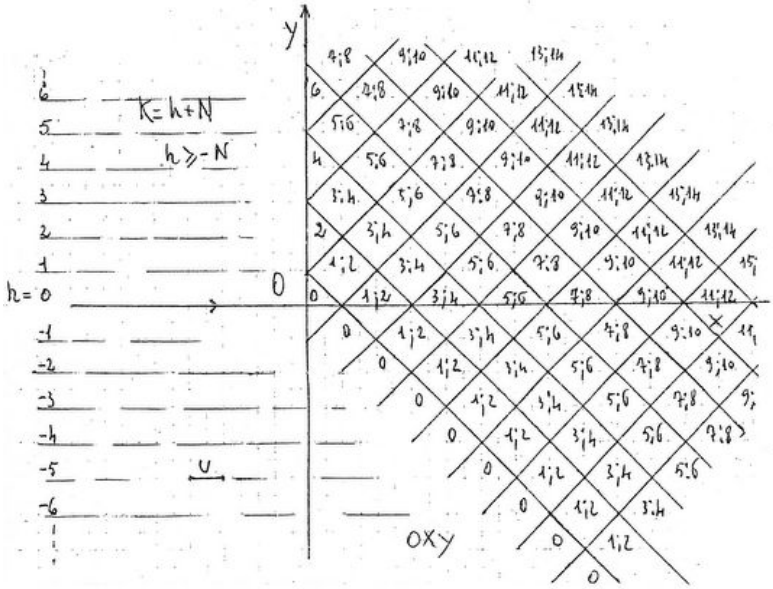
2) $h = 4 \quad e \quad -2 \le x \le -1 \quad \Rightarrow \quad 2 \le x + 4 \le 3 \quad ; \quad k = 2$

3) $h = 3 \quad e \quad 2 \le x \le 3 \quad \Rightarrow \quad 5 \le x + 3 \le 6 \quad ; \quad k = 5$

Osserviamo che nelle tre doppie disuguaglianze dei valori di x (di primo grado), risultando del tipo della doppia disuguaglianza dei valori di x (di secondo grado) presenti nella equazione della rete, sarà facile ricavare i valori di k .

Particolari famiglie della rete

Analizziamo ora una suddivisione della rete in quattro porzioni. Per ciascuna porzione verrà scritto il legame analitico tra le coordinate dei soli suoi punti.
La prima porzione rappresentata nella figura che segue



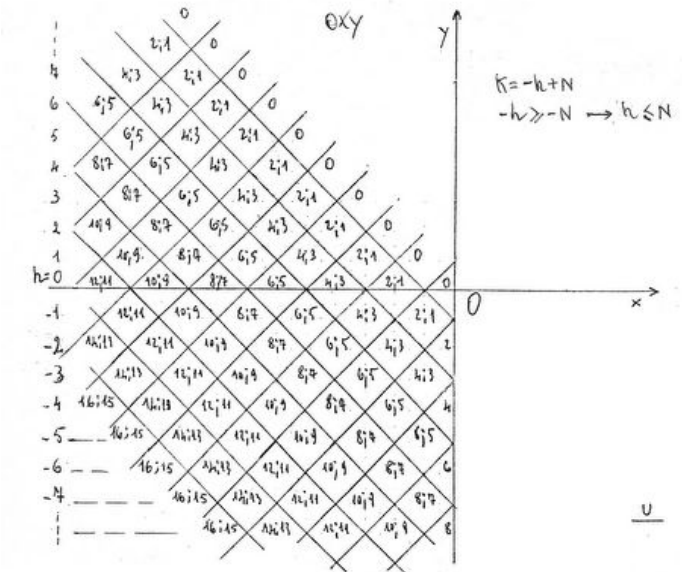
avrà come equazione:

$$y-h=\begin{cases}\pm\left(|x+h|-k_1\right);\\ \\ \pm\left(1+k_2-|x+h|\right);\end{cases}$$

$$N\le x\le 1+N;\quad h\ge -N;\quad k=h+N;\quad N=0,1,2,3,\ldots\ ;$$

$$k_1=k,\text{se } k \text{ è dispari};\quad k_2=k,\text{se } k \text{ è pari o zero.}$$

La seconda porzione rappresentata in figura



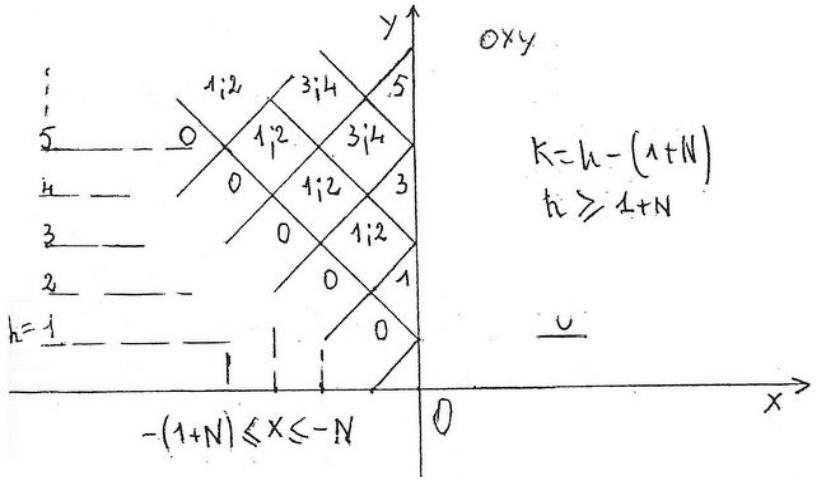
avrà come equazione la seguente:

$$y-h=\begin{cases}\pm\left(|x+h|-k_1\right)\\ \pm\left(1+k_2-|x+h|\right)\end{cases}$$

$$-(1+N)\le x\le -N;\quad h\le N;\quad k=-h+N;\quad N=0,1,2,3,\ldots\ ;$$

$$k_1=k,\text{se } k \text{ è dispari};\quad k_2=k,\text{se } k \text{ è pari o zero.}$$

La terza porzione rappresentata nella seguente figura



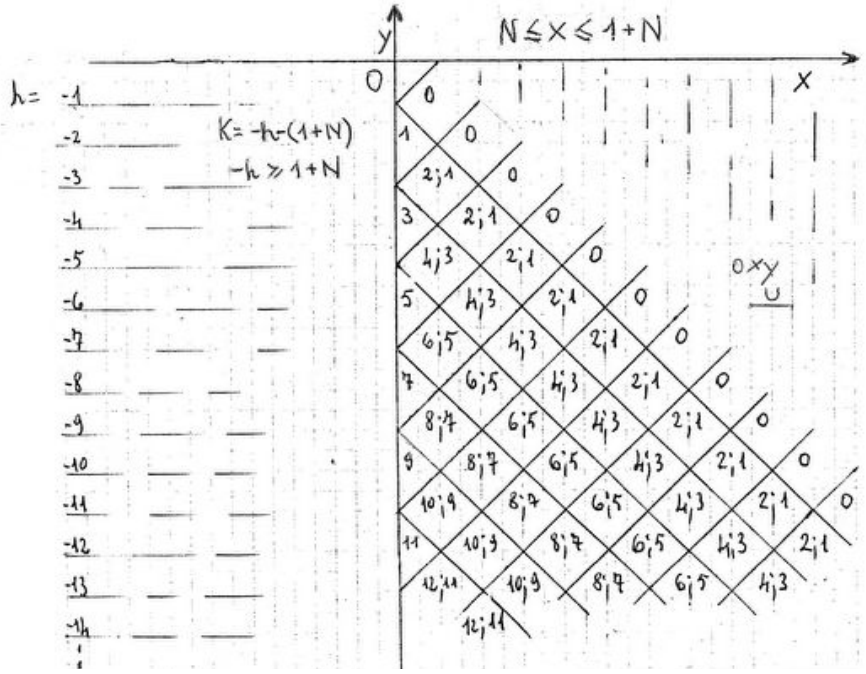
avrà equazione

$$y-h=\begin{cases}\pm\left(|x+h|-k_1\right)\\ \pm\left(1+k_2-|x+h|\right)\end{cases}$$

$$-(1+N)\le x\le -N;\quad h\ge 1+N;\quad k=h-(1+N);\quad N=0,1,2,3,\ldots\ ;$$

$$k_1=k,\text{se } k \text{ è dispari};\quad k_2=k,\text{se } k \text{ è pari o zero.}$$

La quarta porzione rappresentata nella figura



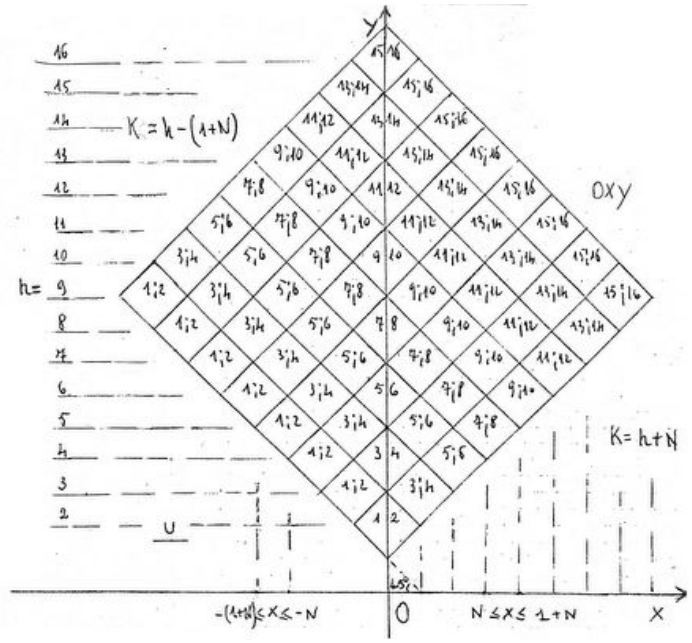
avrà come equazione: $$y-h=\begin{cases}\pm\left(|x+h|-k_1\right);\\ \\ \pm\left(1+k_2-|x+h|\right);\end{cases}$$

$$N\le x\le 1+N;\quad -h\ge 1+N;\quad k=-h-(1+N);\quad N=0,1,2,3,\ldots\ ;$$

$$k_1=k,\text{se } k \text{ è dispari};\quad k_2=k,\text{se } k \text{ è pari o zero.}$$

Equazione del reticolo della dama

Le quattro porzioni descritte potranno essere ora unificate a due a due per formare a loro volta altre famiglie. Nella figura che segue viene rappresentato un diagramma detto reticolo della dama che è la conseguenza di un esempio di unificazione (parziale) di parte della prima porzione con parte della terza porzione.



Vediamo nei dettagli questa metodologia. Dalla porzione 1 si ricava: se $N\le x\le 1+N$ con $N=0,1,2,3,\ldots,7$ allora seguono le due soglie minima e massima di h che risultano essere:

$$h=\begin{cases}h_{\min}=2+N\\ \\ h_{\max}=16-N\end{cases}$$

e quindi il campo di esistenza di h diviene: $2+N\le h\le 16-N$, da cui è possibile ricavare i valori di k, essendo $k=h+N$.

Le soglie di k e il campo di esistenza di k risultano essere i seguenti:

$$k=\begin{cases}k_{\min}=h+k=(2+N)+N=2(1+N)\\ \\ k_{\max}=h+k=(16-N)+N=16\end{cases}$$

quindi $2(1+N)\le k\le 16$.

Dalla porzione 3 si ricava: se $-(1+N) \le x \le -N$ con $N = 0,1,2,3,...,7$ allora seguono le stesse soglie di h e lo stesso campo di esistenza di h: $2+N \le h \le 16-N$, da cui è possibile ottenere anche i valori di k essendo $k = h-(1+N)$.
Le soglie di k e il campo di esistenza di k risultano essere i seguenti:

$$k = \begin{cases} k_{\min} = h-(1+N) = (2+N)-(1+N) = 1 \\ k_{\max} = h-(1+N) = (16-N)-(1+N) = 15-2N \end{cases}$$

quindi $1 \le k \le 15-2N$.
Segue quindi l'equazione del reticolo della dama:

$$y-h = \begin{cases} \pm\left(|x+h|-k_1\right); & N \le x \le 1+N; \quad k = h+N \\ \pm\left(1+k_2-|x+h|\right); & -(1+N) \le x \le -N; \quad k = h-(1+N) \end{cases}$$

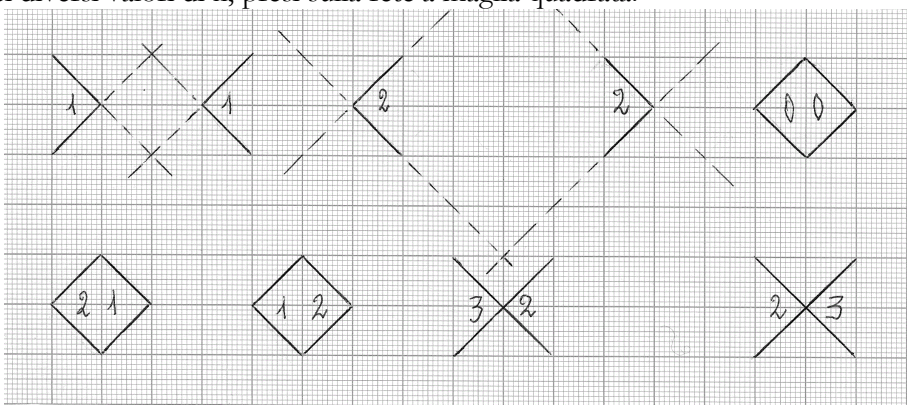
$$2+N \le h \le 16-N; \quad N = 0,1,2,3,...\ 7;$$

$$k_1 = k, \text{se } k \text{ è dispari}; \quad k_2 = k, \text{se } k \text{ è pari o zero}.$$

Nel sistema può capitare che l'intervallo dei valori di x appartenente ad un rigo debba essere associato all'equazione dell'altro rigo. Questo dipenderà dal valore di k, in particolare se k assume valore pari o dispari. Infatti, se nel primo rigo del sistema k risulterà pari, l'abbinamento dovrà essere fatto tra i valori di $N \le x \le 1+N$ e l'equazione del secondo rigo. Mentre se nel secondo rigo il valore di k risulterà dispari, l'abbinamento dovrà essere fatto tra i valori di $-(1+N) \le x \le -N$ e l'equazione del primo rigo.
Con $N = 8,9,...$ il reticolo della dama (8 x 8 quadrati) può essere generalizzato onde poter considerare nel piano Oxy un maggior numero di quadrati, vale a dire una dama grande a piacere.

Complementi

Premesso naturalmente un valore di h, si approfondirà ancora sul valore di k. La figura seguente illustra i casi al variare dei diversi valori di k, presi sulla rete a maglia quadrata.



Per ciascun valore di $k = 1,3,5,...$ le due coppie di segmenti non appartengono al quadrato delimitato dai loro prolungamenti; vi appartengono, invece, nel caso $k = 2,4,6,...$. Se $k = 0$ le due coppie di segmenti delimitano un quadrato. Se, inoltre, due valori di k sono numeri interi consecutivi, dispari il minore e pari il maggiore, ad esempio 1 e 2, per ogni valore di k, ogni coppia di segmenti forma con l'altra coppia due quadrati. Mentre se è pari il minore e dispari il maggiore, ad esempio 2 e 3, per ogni valore di k, i segmenti di ogni coppia sono i prolungamenti dei segmenti dell'altra coppia.

157. Introduzione alla Teoria dei Modelli: il teorema di Löwenheim-Skolem all'ingiù

Paolo Bonicatto
paolo.bonicatto@studenti.unito.it

Sommario

Secondo un'originale definizione, risalente a non più di quarant'anni fa (si veda [2]), la *Teoria dei Modelli* è «Algebra universale più Logica», dove per Algebra universale si intende lo studio delle strutture e per Logica si intende lo studio delle formule logiche e delle regole di inferenza. Un'altra definizione ancora più recente suggerisce invece di vedere la Teoria dei Modelli come «Geometria algebrica meno campi». E' in effetti difficile definire esattamente che cosa significhi Teoria dei Modelli; risulta ancora più arduo demarcare netti confini oltre i quali essa non si spinga. In generale, si potrebbe dire che quasi ogni matematico faccia, più o meno consapevolmente, Teoria dei Modelli. Obiettivo di queste righe è cercare di introdurre il lettore a questo nuovo mondo, dapprima fornendo gli strumenti elementari necessari per la comprensione, poi enunciando e dimostrando quello che è stato uno dei primissimi risultati di Teoria dei Modelli: il cosiddetto *Teorema di Löwenheim-Skolem all'ingiù*.

1 Linguaggi, strutture e formule del prim'ordine

1.1 Linguaggi, strutture

Quasi tutte le persone che hanno incontrato nella loro vita un po' di Matematica hanno sentito parlare di "funzioni" e di "relazioni".

Intuitivamente e informalmente, possiamo dire che, presi due insiemi A e B, una *funzione* $f: A \to B$ è una "legge" che associa ad ogni elemento dell'insieme A uno e un solo elemento di B. Ad esempio, se A è l'insieme degli abitanti di una città e B è l'insieme dei numeri reali positivi, la legge che ad ogni abitante associa la sua altezza (espressa in centimetri) definisce una funzione $f: A \to B$.

D'altra parte, in maniera sempre un po' informale, possiamo dire che una *relazione* n-aria su un insieme A è un qualsiasi sottoinsieme di $A^n := A \times A \times \ldots \times A$: ad esempio, una relazione *unaria* è un qualunque sottoinsieme di A. Una relazione *binaria* è invece un insieme di *coppie* (a, b) di elementi di A. In generale, come già detto, una relazione n-aria su A è un insieme di n-ple $(a_1, \ldots, a_n)$ di elementi di A.

Un *linguaggio* L è un insieme che è unione (disgiunta) di due insiemi L_{rel} e L_{fun}: gli elementi del primo si chiamano simboli per relazioni, gli elementi del secondo simboli per funzioni. Inoltre[1], è parte integrante del linguaggio una funzione $\mathrm{Ar}: L \to \omega$ che associa ad ogni simbolo (per funzione o per relazione) la relativa *arietà*, cioè il numero di "argomenti" della funzione o della relazione. Fissato un linguaggio, per definire una *struttura*, occorre prendere un insieme M (chiamato in maniera originale *dominio della struttura*) e una funzione che associa ad ogni simbolo del linguaggio (sia simboli per relazione che per funzione) una effettiva relazione o funzione su M della arietà giusta. Infine, per *parametro* si intende un elemento $a \in M$ che viene incluso nel linguaggio. Un esempio chiarirà quanto detto finora.

[1] Da ora in poi, per tutto l'articolo, denoteremo con ω l'insieme dei numeri naturali (coerentemente con la teoria degli ordinali).

Esempio
Sia $\mathbb{Z} := \{\dots, -2, -1, 0, +1, +2, \dots\}$ il consueto insieme dei numeri relativi. È abbastanza noto che esso è un gruppo additivo. Vediamo però di esprimere questo fatto nei modi ora esposti. Innanzitutto, il linguaggio è $L := \{0, +, -\}$. Lo 0 può vedersi come un simbolo per funzione 0-aria[2]; $+$ è un simbolo per funzione con arietà due, perché due sono gli "argomenti" che la funzione prende o, detto meglio, $+$ è una funzione $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$; infine, $-$ è un simbolo per funzione 1-aria, infatti $-: \mathbb{Z} \to \mathbb{Z}$. Se ad ogni simbolo ora associamo la sua naturale interpretazione, cioè $(a, b) \mapsto +(a, b) = a + b$ e $a \mapsto -(a) = -a$, allora possiamo affermare che $\mathbb{Z}$ è una struttura nel linguaggio L. Si noti che il linguaggio ora usato viene solitamente indicato come il *linguaggio dei gruppi additivi*, per ovvi motivi.
Lasciamo al volenteroso lettore il non difficile compito di vedere $\mathbb{Z}$ come anello, introducendo un opportuno linguaggio (appunto quello degli anelli: l'elemento 1 può essere incluso nel linguaggio risultando così un parametro.

1.2 Formule
Intuitivamente, ognuno di noi ha una idea più o meno precisa del concetto di *formula*. La Logica però poggia le sue basi su solide fondamenta e avverte il bisogno di formalizzare in maniera pulita e impeccabile anche la definizione di quest'oggetto così comune. In realtà, dietro tutte queste definizioni ricorre assai frequentemente un procedimento induttivo che si è soliti denotare con *induzione sulla sintassi*. Mediante questa tecnica si definiscono i *termini*, che sono oggetti che generalizzano in un certo senso i tradizionali polinomi, e le formule appunto. Una formula è una ben precisa sequenza di simboli (termini, in verità) che rispetta determinate regole logiche. Il procedimento di costruzione delle formule è così ben formalizzato che si può scrivere un semplice algoritmo che permetta a un computer di riconoscere se una data sequenza costituisce o meno una formula. Se t e s sono due termini (si pensi come detto a polinomi) allora $t = s$ è una formula; induttivamente, si dice che, se φ e ψ sono formule, allora anche $\varphi \vee \vee\psi$, $\neg\varphi$, $\exists x \varphi(x)$ sono formule.
Ricordiamo appunto che i quantificatori sono i simboli $\forall$ e $\exists$ che si leggono "per ogni" e "esiste un". In una formula, le variabili che non compaiono sotto l'azione di un quantificatore si chiamano *libere*. Se in una formula non ci sono variabili libere (quindi ogni variabile compare sotto un quantificatore) allora la formula si dice *chiusa* o anche *enunciato*.
Gli enunciati hanno un ruolo privilegiato perché è possibile assegnare loro un valore di verità che dipende ovviamente dalla struttura che consideriamo. Ad esempio, sia φ l'enunciato $\exists x\, x^2 + 1 = 0$ (1 è un parametro): questo enunciato non è vero[3] in $\mathbb{R}$ ma è vero in $\mathbb{C}$. Per dire che un enunciato φ è vero in una struttura M scriveremo $M \vDash \varphi$, che si legge "M *modella* φ". Per dire invece che un enunciato è falso in M si scrive $M \nvDash \varphi$, che si legge "M *non modella* φ". Richiamando l'esempio di sopra, possiamo scrivere $\mathbb{R} \nvDash \varphi$ e $\mathbb{C} \vDash \varphi$.

2 Teorie e modelli: l'equivalenza elementare secondo Tarski
Come si è visto nel paragrafo precedente, una formula in cui non occorrono variabili libere si chiama formula *chiusa*, o anche *enunciato*. Definiamo una *teoria* T come un insieme di enunciati. Inoltre, si dice che la struttura M è un *modello* di T se $M \vDash \varphi$, per ogni $\varphi \in T$, cioé se ogni enunciato di T è vero in M.
Se una teoria T ammette almeno un modello si dice che T è coerente, altrimenti si dice che T è contraddittoria. Introdotte queste definizioni, si può ora presentare una delle nozioni fondamentali della Teoria dei Modelli.

[2] Questo modo di vedere le costanti come particolari funzioni 0-arie è molto utile e usato in Teoria dei Modelli.
[3] Sarebbe opportuno chiarire che cosa intendiamo per "vero": sorvoliamo su questi dettagli tecnici per evitare di annoiare il lettore.

Definizione 2.1. (Equivalenza elementare) Date due strutture M e N, si dice che M è elementarmente equivalente a N e si scrive $M \equiv N$ se

$$M \vDash \varphi \Leftrightarrow N \vDash \varphi \tag{2.1}$$

per ogni enunciato φ senza parametri.

Fu Alfred Tarski, nel 1930, a dare questa apparentemente semplice definizione: sostanzialmente, si identificano due strutture quando gli enunciati (al prim'ordine) veri in una delle due strutture sono tutti e soli quelli veri nell'altra. Inoltre, se le due strutture sono tali che $\mathrm{M} \subseteq \mathrm{N}$ e l'equivalenza della (2.1) si estende a tutti gli enunciati a parametri in M, allora si dice che M è elementarmente equivalente a N *su* M o che M è una *sottostruttura elementare* di N e si scrive $M \preccurlyeq N$.
Come si è detto, questa è una definizione solo *apparentemente* semplice: infatti, è abbastanza difficile dare un esempio non banale di due strutture che siano elementarmente equivalenti. Se consideriamo come struttura l'anello degli interi $\mathbb{Z}$, affermare che una certa struttura M è elementarmente equivalente a $\mathbb{Z}$ significa conoscere tutta la teoria di $\mathbb{Z}$, cioè *tutti* gli enunciati veri in $\mathbb{Z}$, quelli già noti e dimostrati e tutti quelli ancora ignoti e non dimostrati. Come si può intuire, ciò è ben lontano dalle nostre facoltà mentali attuali: si rivela dunque necessario trovare dei modi equivalenti e allo stesso tempo più semplici e utili per maneggiare questa potente nozione di equivalenza elementare. I paragrafi seguenti si muovono proprio in questa direzione.

3 I giochi di Ehrenfeucht-Fraïssé

Pochi anni dopo aver dato la definizione di equivalenza elementare, Tarski, in una conferenza tenuta a Princeton nel 1946, illustrando questa nuova definizione, espresse il desiderio di creare e sviluppare una teoria di «una profondità pari ai moderni concetti di isomorfismo, [...], ora in uso» ([4]).
Ebbene, una simile teoria doveva contenere al suo interno delle condizioni necessarie e sufficienti per l'equivalenza elementare di due strutture date. Il primo a trovare una caratterizzazione utile fu il logico franco-algerino Roland Fraïssé (1920-2008), che espose tali risultati nella sua tesi di laurea (1953). Qualche anno più tardi, A. D. Taimanov, un logico russo, fece le stesse scoperte ma fu solo il polacco Andrzej Ehrenfeucht (1932-vivente) a riformulare il tutto in termini di giochi. Questi giochi sono noti come "giochi di Ehrenfeucht-Fraïssé" o talvolta anche come "back-and-forth games".

3.1 La vera storia di ∀belardo e ∃loisa

Siano A e B due strutture di linguaggio L. Supponiamo ci siano due persone, che chiameremo appunto ∀belardo e ∃loisa, in forma abbreviata ∀ e ∃, che stanno guardando queste due strutture e stanno cercando di confrontarle[4]. I loro pareri sono diametralmente opposti: ∀ ritiene che le due strutture siano diverse, invece ∃ crede che siano uguali. Come si può ben vedere, la loro discussione ha il carattere di un gioco, appunto: il giocatore ∀ vince se trova almeno una differenza tra A e B; in caso contrario, la vittoria va al giocatore ∃.
Ecco come si può giocare: per prima cosa viene dato un numero k, generalmente finito[5], che è la *lunghezza* del gioco. Il gioco, infatti, consiste di k passi: supponiamo ora di pensare alle strutture come due urne contenenti degli elementi. All'i-esimo passo, il giocatore ∀ prende una qualunque delle due strutture e vi sceglie un elemento; il giocatore ∃ risponde scegliendo un elemento

[4] Una nota di colore: la questione sul nome dei due loschi personaggi è tutt'altro che chiusa. Oltre ai già citati ∀belardo e ∃loisa che suggerisce Hodges (vedi [2]), ci sono anche "Spoiler" e "Duplicator" (introdotti da Joel Spencer nei primi anni '90) e anche "Sansone" e "Dalila" (suggeriti da Neil Immerman). Nonostante questi dubbi onomastici, sono tutti stranamente d'accordo nel ritenere Spoiler come il giocatore maschio il cui simbolo è ∀ e Duplicator come la giocatrice ∃.
[5] Si potrebbe scegliere, in realtà, un qualunque ordinale γ.

dall'altra struttura. Si noti che i due giocatori hanno libertà totale di scelta, possono anche ripescare un elemento che avevano già scelto in precedenza. Di più, al giocatore $\exists$ è consentito conoscere e vedere gli elementi che $\forall$ sceglie e entrambi possono segnare e ricordare le proprie mosse precedenti[6]. Alla fine di queste k successive estrazioni, restano individuate le sequenze $\bar{a} = (a_i)$ e $\bar{b} = (b_i)$, che contengono rispettivamente gli elementi di $\forall$ e di $\exists$. La coppia $(\bar{a}, \bar{b})$ è il *gioco*. A questo punto, si può decretare il vincitore: se esiste un isomorfismo $f: A \to B$ tale che $f(\bar{a}) = \bar{b}$ allora ha vinto il difensore, $\exists$. In caso contrario, la vittoria va all'attaccante $\forall$.

Esempio. Vediamo ora un esempio concreto di gioco di Ehrenfeucht-Fraïssé per comparare le strutture di $\mathbb{Q}$ e $\mathbb{Z}$ come gruppi additivi abeliani. Supponiamo $k \geq 2$. Il giocatore $\forall$ può adottare la seguente strategia vincente: sceglie un elemento $a_0 \in \mathbb{Q}$, con $a_0 \neq 0$. In risposta, anche $\exists$ dovrà scegliere un elemento non nullo, altrimenti perde subito (si invita il lettore a riflettere bene sul perché di questa affermazione).
Ora prendiamo $b_0 \in \mathbb{Z}$: sicuramente, esiste un intero n che non divide b_0; tuttavia, il quoziente $\frac{a_0}{n} = a_1 \in \mathbb{Q}$. Allora abbiamo finito: se $\forall$ sceglie $a_1 \in \mathbb{Q}$, il giocatore $\exists$ non ha nessun modo di scegliere un elemento $b_1 \in \mathbb{Z}$ per cui $nb_1 = b_0$ (si noti che ciò è necessario per l'esistenza di un isomorfismo del tipo desiderato). In definitiva, se $k \geq 2$ il giocatore $\forall$ può sempre vincere il gioco[7].

4 Il teorema di Löwenheim-Skolem all'ingiù

4.1 Il test di Tarski-Vaught

Controllare "a mano" quando due strutture sono elementarmente equivalenti è generalmente un'impresa difficile. In effetti, significherebbe controllare che tutti gli enunciati veri in una delle due strutture siano veri anche nell'altra, e viceversa. Si può ben immaginare che ciò è difficilmente controllabile. Il seguente lemma viene in aiuto, offrendo una condizione necessaria e sufficiente per l'equivalenza elementare.

Lemma 1. (*Test di Tarski-Vaught*)
Siano M e N due strutture arbitrarie e sia $M \subseteq N$. Le due seguenti affermazioni sono equivalenti:

(1) $M \preccurlyeq N$;
(2) data una formula $\varphi(x)$ a parametri in M (dove x è una singola variabile), si ha $N \vDash \exists x \varphi(x) \Rightarrow N \vDash \varphi(b)$ per un qualche $b \in M$. □

Vediamo di capire bene che cosa dice questo potente lemma. Prendiamo le due strutture M, N ($M \subseteq N$) e una qualunque formula $\varphi(x)$ a parametri in M. Supponiamo ora che in N ci sia un elemento a per cui $\varphi(a)$ è vera. Dunque, $N \vDash \exists x \varphi(x)$. A questo punto ci dobbiamo chiedere: riusciamo a trovare un testimone (eventualmente diverso da a) della verità di $\varphi(x)$ che non stia solo in N, ma che stia anche in M? Se questa procedura ha esito positivo per ogni formula a parametri in M, allora il Test di Tarski-Vaught ci garantisce che M è una sottostruttura elementare di N.

Non sarebbe difficile dimostrare l'equivalenza delle due affermazioni, ma evitiamo di presentarne qui la dimostrazione.

[6] Per dirlo nel linguaggio della Teoria dei Giochi, si tratta di un *gioco a informazione perfetta*.
[7] Sempre dalla Teoria dei Giochi, il giocatore $\forall$ ha una *strategia vincente*.

4.2 Il teorema di Löwenheim-Skolem all'ingiù

Siamo ora in grado di presentare il *main result* di questo articolo.

Teorema. (*Löwenheim-Skolem all'ingiù*) Sia N una struttura infinita di linguaggio L e sia $A \subseteq N$ un insieme di parametri. Allora esiste una struttura M tale che $A \subseteq M \preccurlyeq N$ e $|M| \leq \max\{|A|, |L|, \omega\}$.

Dimostrazione. La dimostrazione che proponiamo è davvero elementare: l'idea è quella di "costruire" manualmente (mediante un processo induttivo) la struttura di cui dobbiamo mostrare l'esistenza, aggiungendo passo dopo passo gli elementi di cui abbiamo bisogno. Naturalmente, per fare ciò ricorreremo più volte al lemma 1.

Sia dunque $A_0 = A$ e poniamoci la seguente domanda: A_0 è già una sottostruttura elementare di N? Per rispondere, usiamo il test di Tarski-Vaught: per ogni $\varphi(x)$ a parametri in A, se $N \vDash \exists x \varphi(x)$ allora esiste $b \in A$ tale che $N \vDash \varphi(b)$? Se sì, abbiamo evidentemente finito. Supponiamo invece che la risposta sia negativa. Allora costruiamo un insieme A_1 al modo seguente: all'insieme A_0 aggiungiamo tutti gli elementi $b_\varphi \in N$ che sono i testimoni di $N \vDash \exists x \varphi(x)$ (dove $\varphi(x)$ è una formula a parametri in $A_0 = A$): in altre parole, aggiungiamo ad A_0 esattamente quegli elementi che ci mancavano al punto precedente. Formalmente,

$$A_1 = A_0 \cup \{b_\varphi \text{ testimone di } N \vDash \exists x \varphi(x)\}$$

A questo punto, poniamoci nuovamente la domanda: A_1 è una sottostruttura? Se sì, il ciclo termina, altrimenti proseguiamo.

Ebbene, come si può facilmente intuire, al passo i-esimo, costruiamo

$$A_{i+1} = A_i \cup \{b_\varphi \text{ testimone di } N \vDash \exists x \varphi(x)\}$$

dove $\varphi(x)$ è una formula a parametri in A_i.

In conclusione, se consideriamo

$$M := \bigcup_{i \in \omega} A_i$$

abbiamo che M è proprio la sottostruttura elementare cercata (proprio per il test di Tarski-Vaught!). Inoltre, e questo è il risultato sorprendente, M risulta essere numerabile[8], perché unione di insiemi numerabili (gli A_i sono insiemi di formule numerabili). ■

5 Commenti, paradossi, note storiche

Il teorema, come già detto nell'introduzione, è stato uno dei primissimi risultati di quella che sarebbe poi divenuta la Teoria dei Modelli. Come si può ampiamente leggere in [1], una prima "rudimentale" versione del teorema apparve in *Über Möglichkeiten im Relativkalkül* (1915) di Leopold Löwenheim; naturalmente non era ancora nata l'equivalenza elementare, ma il risultato di Löwenheim era già incentrato su una questione di cardinalità dei modelli e dei linguaggi.

Sembra però che la dimostrazione che diede lo stesso Löwenheim fosse errata. Cinque anni dopo, nel 1920, fu Thoralf Skolem a dare una dimostrazione corretta; in seguito, Skolem migliorò la sua prima dimostrazione (che faceva uso dell'assioma della scelta) e nel 1923 riuscì a provare il risultato senza usare l'AC.

Infine, fu Anatoly Ivanovich Maltsev (1936) a dare una dimostrazione completa e corretta del teorema di Löwenheim-Skolem nella sua completa generalità.

[8] In realtà, si potrebbe dare una dimostrazione più generale che fa uso della teoria dei cardinali: in tal caso, si dovrebbe usare la cosiddetta *induzione transfinita* che, nel caso semplice qui proposto, si riduce a induzione usuale.

Ciò che però più colpisce di questo teorema è l'incredulità che esso generò nei suoi stessi scopritori e gli aspetti paradossali che apparentemente lascia.

Per esempio, secondo il teorema di Löwenheim-Skolem all'ingiù, possiamo costruire un modello *numerabile* (!) per fare l'Analisi Matematica. Se come struttura prendiamo $\mathbb{R}$ e come linguaggio un insieme al più numerabile di funzioni ragionevoli, allora il teorema ci garantisce l'esistenza di una sottostruttura $M \preccurlyeq \mathbb{R}$ con $|M| = \omega$.

Un'altra profonda conseguenza (che spinse lo stesso Skolem a rifiutare il risultato come totalmente privo di senso) è passata alla storia come "paradosso di Skolem": esiste un modello M numerabile della teoria degli insiemi. L'aspetto paradossale è che in M è vero l'assioma che permette di definire l'insieme delle parti. Quindi in M c'è un elemento che è (dal punto di vista di M!) l'insieme dei sottoinsiemi dei numeri naturali. Essendo un elemento di M, esso sarà al più numerabile e ciò, si sa, è in contrasto profondo con la teoria classica degli insiemi. L'apparente contraddizione è dovuta al fatto che l'espressione "tutti i sottoinsiemi dei naturali" non ha in M lo stesso significato che ha quotidianamente.
Ancora, una leggenda metropolitana vuole che Thoralf Skolem, oltre a considerare gli insiemi non numerabili «fictions without real existence», rimase sconvolto e scandalizzato per tutta la vita dal fatto che il suo nome venisse associato a un risultato di questo tipo, risultato che lui stesso considerava assurdo e incredibile (cfr. [3]).

Riferimenti bibliografici

[1] JOHN DAWSON, The compactness of first-order logic: from Gödel to Lindström, «History of Philosophy», 1993.
[2] WILFRID HODGES, *A shorter model theory*, Cambridge, Cambridge University Press, 1997.
[3] BRUNO POIZAT, A course in Model Theory. An introduction to contemporary mathematical Logic, Berlin-New York, Springer, 2000.
[4] ALFRED TARSKI, Address at the Princeton University bicentennial conference on problems of Mathematics (December 17-19, 1946), in HOURYA SINACEUR, Bulletin of Symbolic Logic, s.l., 2000.

26 Luglio 2011

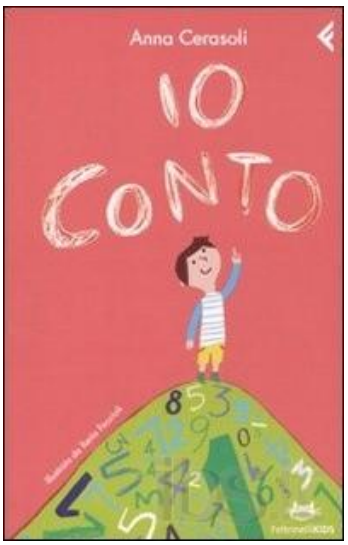
158. Lo scaffale dei libri

Il matematico in giallo" di Carlo Toffalori

Non lasciatevi ingannare dalla copertina: "Il matematico in giallo" di Carlo Toffalori, edito da Guanda, non è l'*alter ego* matematico della signora Fletcher. Infatti, come precisa il sottotitolo "Una lettura scientifica dei romanzi polizieschi", si tratta di un godibile saggio in cui l'autore si propone di illustrare la relazione tra matematica e letteratura gialla, che si rivelerà più profonda e interessante di quanto si possa pensare. Toffalori, professore di Logica Matematica all'Università di Camerino, sceglie di farlo con gli strumenti che gli sono più consoni: quelli dello scienziato. E con la sua lente di ingrandimento esamina i più grandi detective della letteratura partendo da Auguste Dupin di Edgar Allan Poe, passando per Sherlock Holmes e Hercule Poirot, Nero Wolfe e Ellery Queen. Forse stupisce trovare tra i tanti investigatori logici e scientifici chi come Maigret è il meno matematico di tutti; proprio lui però secondo l'autore interpreta al meglio il modo di lavorare di un matematico, con il suo rimuginio lento e talora ossessivo su un problema. Nella maggior parte dei romanzi la figura del matematico, sia esso investigatore o criminale, appare stereotipata e lontana dalla realtà: per esempio annovera sempre tra le sue passioni scacchi, bridge e enigmistica o rispecchia la tipica immagine del genio e del professore, non avvenente, distratto, impacciato e poco socievole, ma perfettamente a proprio agio nello studio della sua materia. Tuttavia il quadro che ne emerge è piuttosto vario: si parla di crittografia e informatica teorica, dei Teoremi di Goedel e di scacchi; si affronta il tema del rapporto tra uomini e macchine (grazie ai romanzi di Asimov). L'autore dimostra di essere un ottimo divulgatore presentando ai lettori anche argomenti più specialistici come l'Ultimo Teorema di Fermat e la Congettura di Goldbach con il taglio del romanzo giallo, con la suspence degna di storie del genere. Quindi, amanti di polizieschi e appassionati di matematica non fatevi sfuggire questa piacevole lettura.

Silvia Vermicelli

Anna Cerasoli, *Io conto*, Feltrinelli



"Quando finisce la scuola e cominciano le vacanze mi sento felice… ma quando ritorniamo mi viene un po' di nostalgia della scuola e vorrei rivedere i miei compagni." Così comincia un altro anno di scuola e un altro libro di Anna Cerasoli, un altro racconto di un giovane protagonista alle prese con le piccole angosce della scuola, i dubbi e le scoperte della matematica. Il libro è in buona parte dedicato alle frazioni, può essere un utile strumento non solo per i giovani lettori ma anche per maestri/e che possono trovarci utili spunti laboratoriali e per i genitori che vi spossono trovare idee per agevolare il rapporto con la matematica dei loro figli.

magazine
MATEMATICAMENTE.IT
Rivista trimestrale di matematica per curiosi e appassionati distribuita gratuitamente sul sito

Anno 5 Numero 15 MAGGIO 2011
Registrazione n. 953 del 19.12.2006 – Tribunale di Lecce
ISIN ISSN 2035-0449
Direttore responsabile Antonio Bernardo
antoniobernardo@matematicamente.it