LA LOGICA DELLE EQUAZIONI

Carlo Toffalori (Camerino)

Educare alla razionalità. In ricordo di Paolo Gentilini

Sestri Levante, 9-11 giugno 2016

L'Algebra nelle Indicazioni Nazionali: risolvere equazioni

- l'utilità delle equazioni,
- indeterminate, coefficienti, parametri,
- $\sqrt{2}, \Phi, i, \pi$, ...

La Logica nelle Indicazioni Nazionali: solo tra le righe

- interdisciplinarità,
- Euclide, assiomi, postulati e teoremi,
- l'infinito,
- algoritmi.

Le obiezioni all'insegnamento della Logica

- D'accordo ragionare e dimostrare…
- … ma senza esagerare: assurdo imparare le regole della logica.

Nuove parole d'ordine: non astrarre, ma ***"modellizzare"***.

Per apprendere la logica bastano le equazioni (che del resto sono già abbastanza noiose).

Ma è davvero così? Thomas Mann, *Altezza Reale*

“ – E i suoi studi, signorina? E’ permesso informarsi? Matematica, è vero? Non è molto difficile? Non è uno sforzo terribile, per il cervello?

- Niente affatto. Non saprei immaginare niente di più divertente. E’ ***un gioco dell’aria****, per dir così. Anzi, addirittura fuori dell’aria.”*

Tornando alle equazioni

- personaggi e interpreti,
- l'importanza del contesto

$$1 + 1 = 0?$$

Il problema del mercante di bestiame di ***Eulero***

Un mercante di bestiame ha speso complessivamente a una fiera 1770 talleri per comprare tori e cavalli, 31 talleri per ogni toro e 21 talleri per ogni cavallo. Quanti tori e cavalli ha acquistato?

Semplice! $31 \cdot x + 21 \cdot y = 1770$, da cui $y = \frac{1770-31 \cdot x}{21}$.

O no? Si cercano soluzioni non razionali, ma intere positive.

Dedekind, 1888, *Che cosa sono e che sono dovrebbero essere i numeri*, le identità fondamentali di $(\mathbb{N}, +, \cdot, 1)$ (e non solo!)

(1) $x + y = y + x$,
(2) $x + (y + z) = (x + y) + z$,
(3) $x \cdot 1 = x$,
(4) $x \cdot y = y \cdot x$,
(5) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
(6) $x \cdot (y + z) = x \cdot y + x \cdot z$.

Altre se ne aggiungono, come $(x + 1)^2 = x^2 + 2 \cdot x + 1$. Ma almeno questa si dimostra a partire dalle precedenti (esercizio…).

Due problemi

(a) E' vero che ogni identità valida in $(\mathbb{N}, +, \cdot, 1)$ si ***dimostra*** a partire da (1)-(6)?

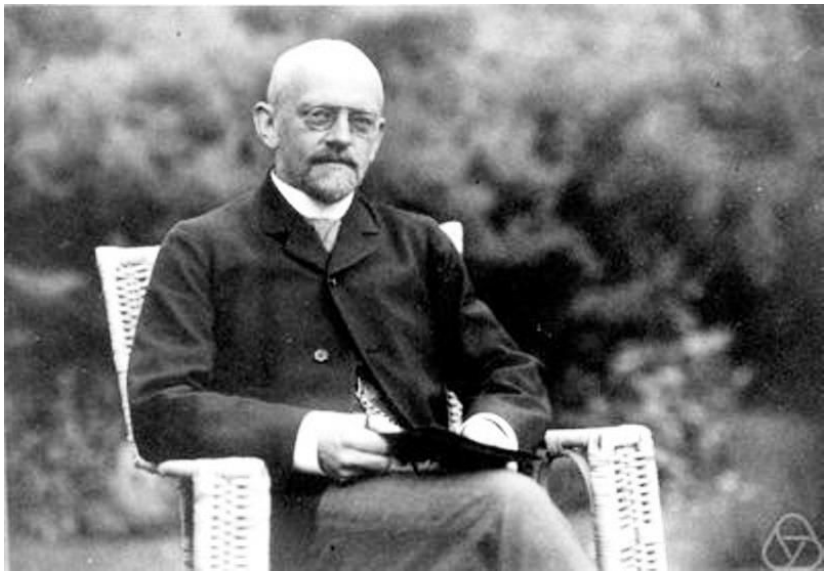
(b) Esiste un algoritmo per distinguere, tra le equazioni polinomiali a coefficienti interi positivi, quelle identicamente vere in $(\mathbb{N}, +, \cdot, 1)$?

Da chiarire preventivamente: che cosa è una ***dimostrazione***?

Nel nostro caso, una sequenza ordinata finita di identità di $(\mathbb{N}, +, \cdot, 1)$ che

- muove da quelle di (1)-(6),
- si conclude con quella cercata,
- usa le seguenti regole per deduzioni elementari, per ogni scelta di polinomi f, g, h, f', g' a coefficienti interi (positivi e non solo)

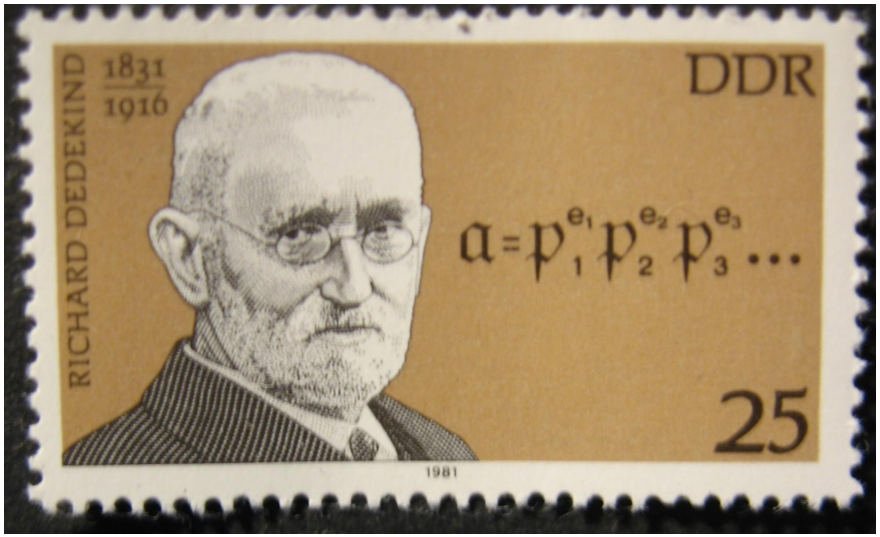
i) $f = f$,
ii) $g = f$ **da** $f = g$,
iii) $f = h$ **da** $f = g$ e $g = h$,
iv) $f + g = f' + g'$ **da** $f = f'$ e $g = g'$,
v) $f \cdot g = f' \cdot g'$ **da** $f = f'$ e $g = g'$.



Su questa base la riduzione di un polinomio in ***forma normale***. Di più, per f, g polinomi a coefficienti interi (positivi)

(a) $f = g$ è un'identità se e solo se f e g hanno la stessa forma normale
(b) un algoritmo per riconoscere le identità di $(\mathbb{N}, +, \cdot, 1)$.

In conclusione (ISS1-6) costituiscono una base assiomatica per le identità soddisfatte da $(\mathbb{N}, +, \cdot, 1)$ – la così detta *teoria equazionale* di $(\mathbb{N}, +, \cdot, 1)$ – e sono capaci di provare quelle valide e di confutare quelle fallaci.



Ancora Dedekind:

(7) $1^x = 1$,

(8) $x^1 = x$,

(9) $x^{y+z} = x^y \cdot x^z$,

(10) $(x \cdot y)^z = x^z \cdot y^z$,

(11) $(x^y)^z = x^{y \cdot z}$.

Vere con (1)-(6) in $(\mathbb{N}, +, \cdot, 1, exp)$ se poniamo, per x, y interi positivi, $exp(x, y) = x^y$.

Il problema della scuola superiore (***High School Problem***)

(a) E' vero che ogni identità (anche esponenziale) valida in $(\mathbb{N}, +, \cdot, 1, exp)$ si ***dimostra*** a partire da (1)-(11)?

E ancora…

(b) Esiste un algoritmo per distinguere, tra le equazioni esponenziali a coefficienti interi positivi, quelle identicamente vere in $(\mathbb{N}, +, \cdot, 1, exp)$?

Lecito dedurre, per f, g, f', g' polinomi esponenziali a coefficienti interi (positivi), anche

vi) $f^g = f'^{g'}$ **da** $f = f'$ e $g = g'$.

La risposta di Alex Wilkie

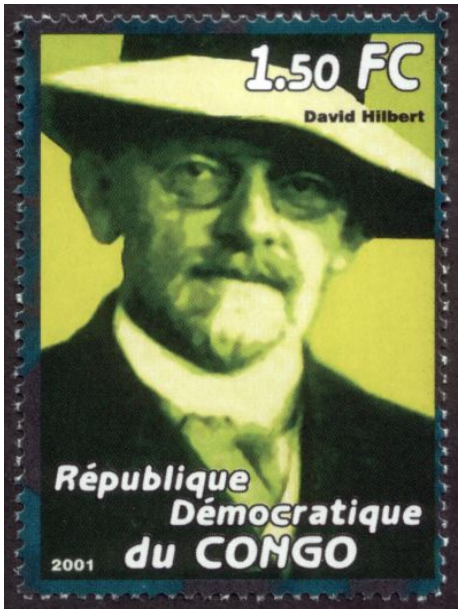
$$W(x,y):\ ((1+x)^y+(1-x+x^2)^y)^x\cdot((1+x^3)^x+(1+x^2+x^4)^x)^y=$$
$$=((1+y)^x+(1+x+x^2)^x)^y\cdot((1+x^3)^y+(1+x^2+x^4)^y)^x.$$

- vera in $(\mathbb{N},+,\ \cdot,1,exp)$,
- non dimostrabile da (1)-(11).

In compenso (Macintyre, Gurevic) un algoritmo per (b), ma servono infiniti assiomi!

Equazioni diofantee: coefficienti interi, alla ricerca di soluzioni intere!

- Il problema del mercante di bestiame di Eulero
- L'equazione di Bombelli $x^3 - 15\,x - 4 = 0$
- Il teorema di Pitagora e le terne pitagoriche $x^2 + y^2 = z^2$
- L'Ultimo Teorema di Fermat $x^n + y^n = z^n, n \geq 3$
- $\sqrt{2}$, Φ, i, …



H10, il Decimo Problema di Hilbert (1900)

- (in termini moderni) *determinare un algoritmo che, per ogni polinomio a coefficienti interi, stabilisca se quel polinomio ammette o no radici intere.*

Qualunque grado, qualunque numero di incognite!

Il caso del grado 1

$$a_1 x_1 + \cdots + a_n x_n = b$$

Ci sono soluzioni intere se e solo se il massimo comune divisore di $a_1, \ldots, a_n$ divide b (l'uso dell'algoritmo euclideo).

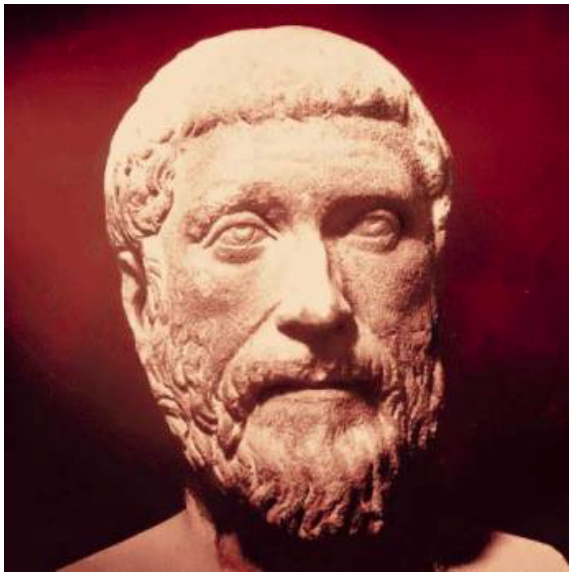
Il caso di un'unica indeterminata

$$a_0 + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_n \cdot x^n = 0$$

con n intero positivo, $a_n \neq 0$.

- Se $a_0 = 0$, c'è la soluzione nulla $x = 0$.
- Altrimenti le soluzione ***razionali*** (in particolare le ***intere***), se esistono, si trovano tra le frazioni $\frac{p}{q}$ con p, q interi, p divisore di a_0 e q divisore di a_n.

Basta (?) un controllo per forza bruta, esteso a tutti questi divisori.



***Equazioni quadratiche**: il caso di un'equazione di grado 2 e 2 indeterminate x, y della forma*

$$a \cdot x^2 + b \cdot y = c$$

con a, b, c interi positivi.

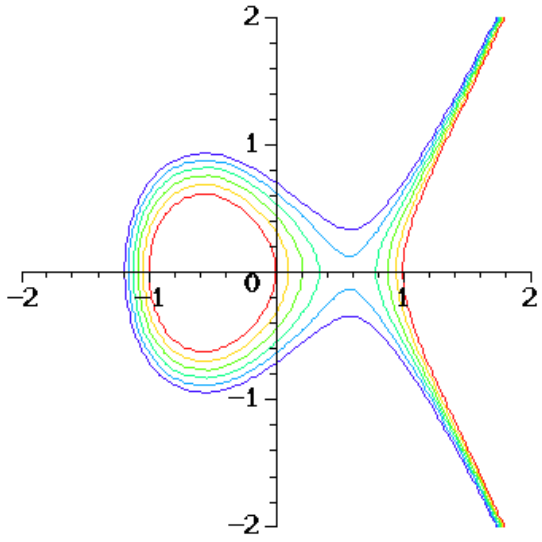
Idea: trova le soluzioni intere di $a \cdot X + b \cdot y = c$ e poi controlla quando X è un quadrato (modulo b). Facile a dirsi. E a farsi?

La risposta generale a H10 (M. Davis, H. Putnam, J. Robinson, Y. Matijasevic, DMPR, 1970): ***nessun algoritmo!***

Di nuovo il ruolo della funzione esponenziale…

Di mezzo (1936, Church, Turing) una risposta ai seguenti interrogativi:

- quali sono i problemi con o senza algoritmo di soluzione,
- che cosa è un calcolatore, o un programma di calcolatore.



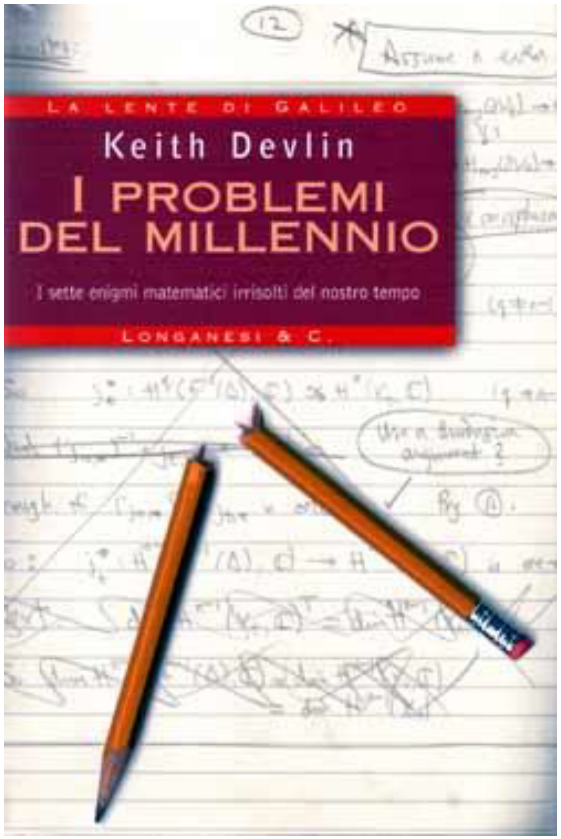
Tornando ai casi particolari

- ***Grado 1***: l'algoritmo euclideo delle divisioni successive (ottimo ed efficiente)
- ***Un'unica indeterminata***: non facile trovare i divisori di un intero…
- ***Due indeterminate, grado 2,*** $a \cdot x^2 + b \cdot y =$: analoghe difficoltà, almeno allo stato attuale delle conoscenze

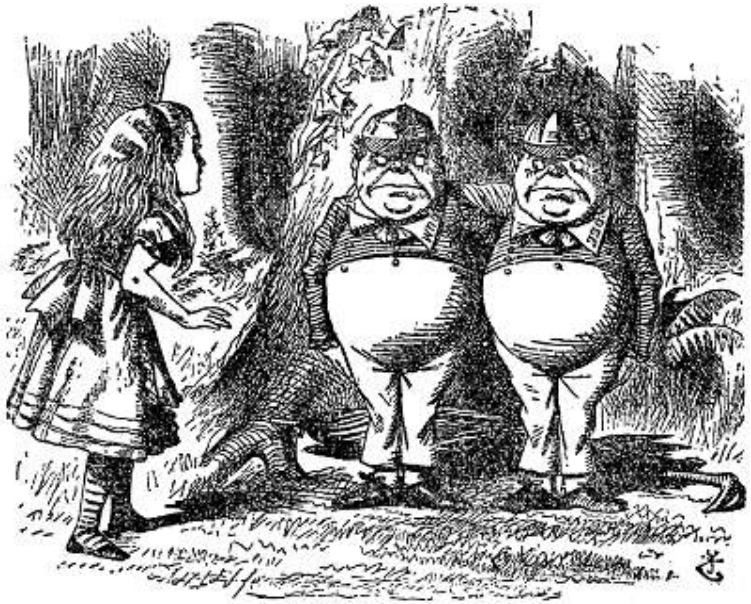
L'importanza di correre e far presto…

- P = classe dei problemi veloci da risolvere
- NP = classe dei problemi veloci da risolvere ***con un po' di aiuto***

Chiaramente P è contenuta in NP.



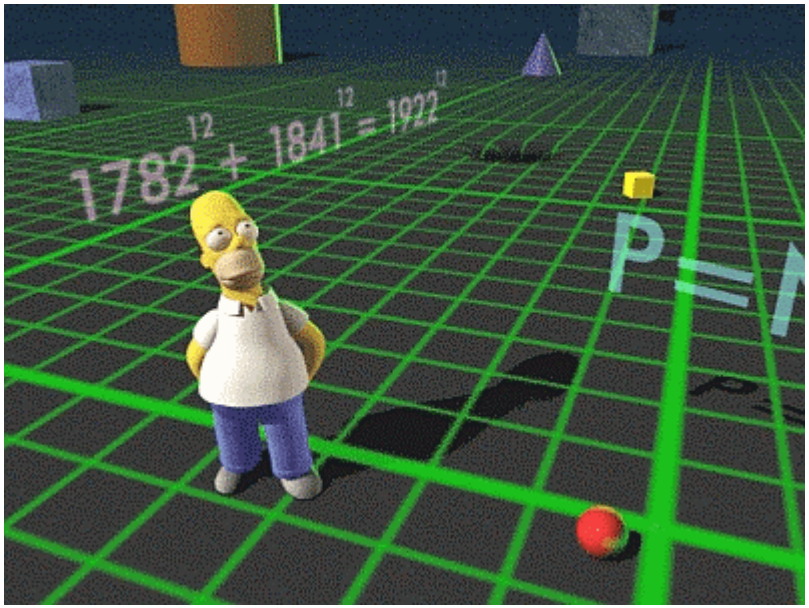
Un ***problema del millennio*** (2000): P = NP?



Due casi possibili:

- o si trova ***qualche*** problema in NP e non in P, e quindi P è diversa da NP…
- oppure ***tutti*** i problemi di NP stanno in P, e allora P = NP.

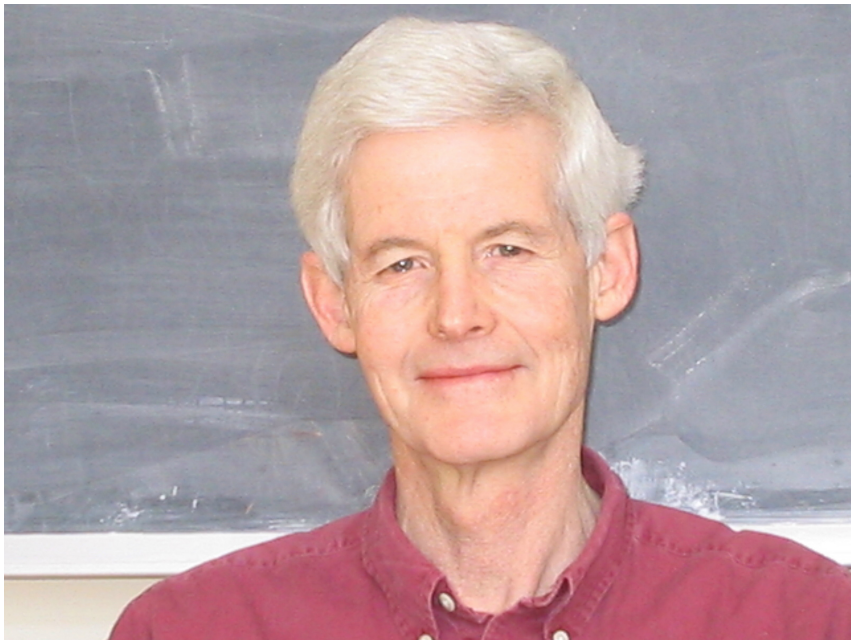
"That's logic!" (L. Carroll)



Eppure problemi ***NP-completi***

- in NP
- e, se in P, capaci di implicare P = NP.

Gli altri si riducono a loro.



Esempi (l'ubiquità della logica…)

- Il primo: *SAT* (Cook, 1970): una questione di equazioni della logica
- Tra gli altri: ***Equazioni quadratiche*** (Manders-Adleman, 1976)

Così difficile come P = NP

Spunti sparsi ma rilevanti di una Logica che

- emerge dalle equazioni e le chiarisce,
- non ingabbia né reprime,
- anzi stimola la fantasia, la sorpresa, il gusto della scoperta e della discussione.

Come tale, da consigliare

- certamente nella formazione dei docenti
- e, a loro discrezione, nelle forme adeguate, nell'insegnamento.