Prefazione al 10^{o} problema di Hilbert

Eugenio G. Omodeo
Università degli Studi di Trieste

Trieste, 01.03.2016

लीलावती

Un quinto di uno sciame di api si posò su un fiore di kudamba, un terzo su un fior di silindha. Tre volte la differenza tra i due numeri volò sui fiori di un kutuja, e rimase solo un'ape che si librò qua e là nell'aria, ugualmente attratta dal grato profumo di un gelsomino e di un pandamus. Dimmi tu ora, donna affascinante, qual era il numero delle api?

Poesia tratta da "Līlāvāti" di Bhaskara (1114-1185)

$$x = \frac{x}{5} + \frac{x}{3} + 3\left(\frac{x}{3} - \frac{x}{5}\right) + 1$$

Esempio di Davis "One equation to rule them all" (1968)

L'equazione

$$9\,(u^2 + 7\,v^2)^2 - 7\,(r^2 + 7\,s^2)^2 \;=\; 2$$

ha soluzioni intere non-negative

?

Esempio di Davis "One equation to rule them all" (1968)

L'equazione

$$9\,(u^2+7\,v^2)^2-7\,(r^2+7\,s^2)^2 \;=\; 2$$

ha soluzioni intere non-negative, oltre a quella banale $\boldsymbol{u}=\boldsymbol{r}=1$, $\boldsymbol{v}=\boldsymbol{s}=0$?

Esempio di Davis "One equation to rule them all" (1968)

L'equazione

$$9\,(u^2+7\,v^2)^2-7\,(r^2+7\,s^2)^2 \;=\; 2$$

ha soluzioni intere non-negative, oltre a quella banale $\boldsymbol{u}=\boldsymbol{r}=1$, $\boldsymbol{v}=\boldsymbol{s}=0$?

Sí (1971 / 1972); c'è la

$$\begin{array}{rclrcl} \boldsymbol{u} & = & 525692038369576\,, & \boldsymbol{r} & = & 2484616164142152\,, \\ \boldsymbol{v} & = & 1556327039191013\,, & \boldsymbol{s} & = & 1381783865776981\,. \end{array}$$

Scaletta

Il X problema di Hilbert

David Hilbert avanzò 23 problemi in occasione del *Congresso internazionale dei matematici* a Parigi, l'8 agosto 1900

Il X problema di Hilbert

David Hilbert avanzò 23 problemi in occasione del *Congresso internazionale dei matematici* a Parigi, l'8 agosto 1900

10. Entscheidung der Lösbarkeit einer diophantischen Gleichung Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffizienten sei vorgelegt: *Man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.* [2]

Il X problema di Hilbert (Traduzione)

David Hilbert avanzò 23 problemi in occasione del *Congresso internazionale dei matematici* a Parigi, l'8 agosto 1900

10. Determinazione della risolubilità di un'equazione diofantea

Data un'equazione diofantea in qualsiasi numero d'incognite e a coefficienti interi razionali: *Ideare un procedimento per mezzo del quale si possa stabilire, in un numero finito di operazioni, se l'equazione sia risolubile negli interi razionali.* [2]

Che significa *intero razionale* ? (Doveroso richiamo)

Che significa *intero razionale* ? (Doveroso richiamo)

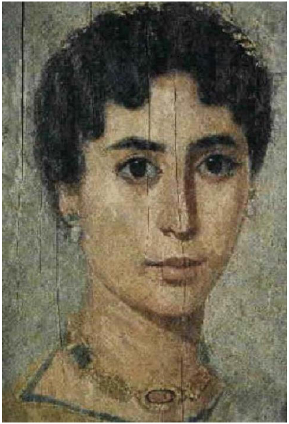
$$
\begin{tikzcd}
 & \text{numeri complessi } (\mathbb{C}) & \\
\text{numeri reali } (\mathbb{R}) \arrow[ur] & & \text{numeri algebrici} \arrow[ul] \\
\text{numeri razionali } (\mathbb{Q}) \arrow[u] \arrow[urr] & & \text{interi algebrici} \arrow[u] \\
 & \text{interi razionali } (\mathbb{Z}) \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

Retrospettiva:


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obseruationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inuentum nouum, collectum
ex varijs eiusdem D. de FERMAT Epistolis.

TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.

(Diofanto, ca. 200 / 284 d.C.)



(Ipazia, ca. 370 / 415 d.C.)

Osservazioni sul X di Hilbert

- Anche se H. non lo dice, secondo ogni verosimiglianza storica, si riferiva ad equazioni polinomiali.
-
-
-

Osservazioni sul X di Hilbert

- Anche se H. non lo dice, secondo ogni verosimiglianza storica, si riferiva ad equazioni polinomiali.
- Perché H. non richiede *coefficienti* in $\mathbb{Q}$? Come vediamo dal problema delle api, ciò non avrebbe fatto una vera differenza.
-
-

Osservazioni sul X di Hilbert

- Anche se H. non lo dice, secondo ogni verosimiglianza storica, si riferiva ad equazioni polinomiali.
- Perché H. non richiede *coefficienti* in $\mathbb{Q}$? Come vediamo dal problema delle api, ciò non avrebbe fatto una vera differenza.
- Perché H. non richiede *soluzione* su $\mathbb{R}$? Se lo avesse fatto, il problema sarebbe stato positivamente risolto da Tarski ca. nel 1930. (V. [4]).
-

Osservazioni sul X di Hilbert

- Anche se H. non lo dice, secondo ogni verosimiglianza storica, si riferiva ad equazioni polinomiali.
- Perché H. non richiede *coefficienti* in $\mathbb{Q}$? Come vediamo dal problema delle api, ciò non avrebbe fatto una vera differenza.
- Perché H. non richiede *soluzione* su $\mathbb{R}$? Se lo avesse fatto, il problema sarebbe stato positivamente risolto da Tarski ca. nel 1930. (V. [4]).
- Perché H. non pone limitazioni sul grado, cosí come non ne pone sul num. delle incognite? Se avesse limitato il grado a 2, il problema sarebbe stato positivamente risolto da Siegel nel 1972. (V. [5]).

Come intendere il X di Hilbert (v. Bjorn Poonen)

H10: Trovare un algoritmo che risolva il seguente problema:

dato: $F(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$

fornire: Sí o No a seconda che esista o meno un $\vec{v} \in \mathbb{Z}^m$ con $F(\vec{v}) = 0$.

(Non occorre dunque produrre una soluzione; solo stabilire se c'è)

Come intendere il X di Hilbert (v. Bjorn Poonen)

H10: Trovare un algoritmo che risolva il seguente problema:

dato: $F(x_1, \dots, x_m) \in \mathbb{Z}[x_1, \dots, x_m]$

fornire: SÍ o NO a seconda che esista o meno un $\vec{v} \in \mathbb{Z}^m$ con $F(\vec{v}) = 0$.

(Non occorre dunque produrre una soluzione; solo stabilire se c'è)

Piú in generale, potremmo chiedere un algoritmo che 'risolva' un sistema di equazioni polinomiali, considerando che ciò risulta equivalente a risolverne una (visto che non abbiamo limitazioni sul grado). Infatti:

$$F_1 = \cdots = F_h = 0 \quad \longleftrightarrow \quad F_1^2 + \cdots + F_h^2 = 0 \ .$$

Esempio di responsi ad *istanze* del X di Hilbert

Sono, rispettivamente, ri- / irre- / ri-solubile le equazioni:

$$\begin{array}{rcl} x^2 + y^2 & = & z^2 \\ x^2 + 1 & = & 0 \\ x^4 \pm 1 & = & 0 \end{array}$$

e perciò dovrà essere Sí / No / Sí il responso per i polinomi

$$\begin{array}{rcl} x^2 + y^2 & - & z^2 \\ x^2 + 1 & & \\ x^8 - 1 & & . \end{array}$$

Ma ogni responso deve provenire da un *metodo generale* !

'Appiattimento' del X di Hilbert — Riduzione al 4^{o} grado

Esercizio. (Risolto in [3]) Mostrare che il X di Hilbert potrebbe, senza perdita di generalità, essere riferito a sistemi (= congiunzioni) di equazioni delle due forme

$$\begin{array}{rcl} \alpha & = & \beta\,\gamma\,, \\ \alpha & = & \beta+\gamma\,, \end{array}$$

dove α, β, γ stanno a rappresentare particolari numeri naturali (ad es. 0 ed 1) oppure incognite.

'Appiattimento' del X di Hilbert   Riduzione al $4^{\rm o}$ grado

Esercizio. (Risolto in [3]) Mostrare che il X di Hilbert potrebbe, senza perdita di generalità, essere riferito a sistemi (= congiunzioni) di equazioni delle due forme

$$\begin{array}{rcl} \alpha & = & \beta\,\gamma\,, \\ \alpha & = & \beta+\gamma\,, \end{array}$$

dove α, β, γ stanno a rappresentare particolari numeri naturali (ad es. 0 ed 1) oppure incognite.

(E se invece della moltiplicaz. usassi l'elevamento al quadrato ?)

Anche questo un'istanza del X di Hilbert ?

Che dire di questo sistema ?

$$\begin{cases} (x+1)^{3+w} + (y+1)^{3+w} = (z+1)^{3+w} \\ x \geqslant 0 \;,\; y \geqslant 0 \;,\; z \geqslant 0 \;,\; w \geqslant 0 \end{cases}$$

Anche questo un'istanza del X di Hilbert ?

Che dire di questo sistema ?

$$\begin{cases} (x+1)^{3+w} + (y+1)^{3+w} = (z+1)^{3+w} \\ x \geqslant 0 \ , \ y \geqslant 0 \ , \ z \geqslant 0 \ , \ w \geqslant 0 \end{cases}$$

In base al famigerato *grande teorema di Fermat* (1637 $\rightsquigarrow$ 1994), questo *non* ha soluzione

Anche questo un'istanza del X di Hilbert ?

Che dire di questo sistema ?

$$\begin{cases} (x+1)^{3+w} + (y+1)^{3+w} = (z+1)^{3+w} \\ x \geqslant 0 \ , \ y \geqslant 0 \ , \ z \geqslant 0 \ , \ w \geqslant 0 \end{cases}$$

In base al famigerato *grande teorema di Fermat* (1637 $\rightsquigarrow$ 1994), questo *non* ha soluzione: *avrebbe potuto rivelarcelo l'algoritmo richiesto da Hilbert*?

Anche questo un'istanza del X di Hilbert ?

Che dire di questo sistema ?

$$\begin{cases} (x+1)^{3+w} + (y+1)^{3+w} = (z+1)^{3+w} \\ x \geqslant 0 \;,\; y \geqslant 0 \;,\; z \geqslant 0 \;,\; w \geqslant 0 \end{cases}$$

In base al famigerato *grande teorema di Fermat* (1637 $\rightsquigarrow$ 1994), questo *non* ha soluzione: *avrebbe potuto rivelarcelo l'algoritmo richiesto da Hilbert*?

Difficoltà 1: incognite in $\mathbb{N}$;

Anche questo un'istanza del X di Hilbert ?

Che dire di questo sistema ?

$$\begin{cases} (x+1)^{3+w} + (y+1)^{3+w} = (z+1)^{3+w} \\ x \geqslant 0 \;,\; y \geqslant 0 \;,\; z \geqslant 0 \;,\; w \geqslant 0 \end{cases}$$

In base al famigerato *grande teorema di Fermat* (1637 $\rightsquigarrow$ 1994), questo *non* ha soluzione: *avrebbe potuto rivelarcelo l'algoritmo richiesto da Hilbert*?

Difficoltà 1: incognite in $\mathbb{N}$;

Difficoltà 2: l'incognita w ad esponente.

Teorema di Lagrange dei quattro quadrati (ca. 1770)

Ogni numero naturale può essere rappresentato come somma di quattro quadrati perfetti, i.e.:

$$(\forall b \in \mathbb{N}\ \exists z_1 \in \mathbb{Z}\ \exists z_2 \in \mathbb{Z}\ \exists z_3 \in \mathbb{Z}\ \exists z_4 \in \mathbb{Z} \mid b = z_1^2 + z_2^2 + z_3^2 + z_4^2)\,.$$

Grazie a ciò possiamo aggirare la prima difficoltà e riferire l'enigma di Fermat al seguente '*polinomio esponenziale*':

$$\left(1 + \sum_{i=1}^{4} x_i^2\right)^{3+\sum_{i=1}^{4} w_i^2} + \left(1 + \sum_{i=1}^{4} y_i^2\right)^{3+\sum_{i=1}^{4} w_i^2} - \left(1 + \sum_{i=1}^{4} z_i^2\right)^{3+\sum_{i=1}^{4} w_i^2}\,.$$

Semplificazione, solo apparente, del X di Hilbert

H10: Trovare un algoritmo che risolva il seguente problema:

dato: $F(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$

fornire: Sí o No a seconda che esista o meno un $\vec{v} \in \mathbb{N}^m$ con $F(\vec{v}) = 0$.

☞

Semplificazione, solo apparente, del X di Hilbert

H10: Trovare un algoritmo che risolva il seguente problema:

dato: $F(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$

fornire: Sí o No a seconda che esista o meno un $\vec{v} \in \mathbb{N}^m$ con $F(\vec{v}) = 0$.

☞

Esercizio: Spiegare perché la semplificazione or ora proposta non svisa il X problema. (Ma se Hilbert lo avesse riferito a $\mathbb{Q}$ o a $\mathbb{R}$?)

Semplificazione, solo apparente, del X di Hilbert

H10: Trovare un algoritmo che risolva il seguente problema:

dato: $F(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$

fornire: SÍ o NO a seconda che esista o meno un $\vec{v} \in \mathbb{N}^m$ con $F(\vec{v}) = 0$.

☞

Esercizio: Spiegare perché la semplificazione or ora proposta non svisa il X problema. (Ma se Hilbert lo avesse riferito a $\mathbb{Q}$ o a $\mathbb{R}$?)

Esercizio: Potremmo triplicare, anziché quadruplicare, il numero delle incognite ?

Semplificazione, solo apparente, del X di Hilbert

H10: Trovare un algoritmo che risolva il seguente problema:

dato: $F(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$

fornire: SÍ o NO a seconda che esista o meno un $\vec{v} \in \mathbb{N}^m$ con $F(\vec{v}) = 0$.

Esercizio: Spiegare perché la semplificazione or ora proposta non svisa il X problema. (Ma se Hilbert lo avesse riferito a $\mathbb{Q}$ o a $\mathbb{R}$?)

Esercizio: Potremmo triplicare, anziché quadruplicare, il numero delle incognite ? (V. teor. dei 3 quadrati di Legendre–Gauss)

Soluzione, ahimè illusoria, del X di Hilbert

Acquisizione dato: Il solito pol. $F(x_1, \ldots, x_m)$ a coefficienti in $\mathbb{Z}$;

Soluzione, ahimè illusoria, del X di Hilbert

Acquisizione dato: Il solito pol. $F(x_1, \ldots, x_m)$ a coefficienti in $\mathbb{Z}$;

Generazione: Enumera, in maniera *esaustiva*—quanto meno in linea di principio—, le m-uple $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ di valori assegnabili alle variabili;

Soluzione, ahimè illusoria, del X di Hilbert

Acquisizione dato: Il solito pol. $F(x_1, \ldots, x_m)$ a coefficienti in $\mathbb{Z}$;

Generazione: Enumera, in maniera *esaustiva*—quanto meno in linea di principio—, le m-uple $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ di valori assegnabili alle variabili;

Valutazione: Per ogni m-upla, effettua la sostituzione $x_i \rightsquigarrow \boldsymbol{v}_i$ per $i = 1, \ldots, m$ e quindi calcola $F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$;

Soluzione, ahimè illusoria, del X di Hilbert

Acquisizione dato: Il solito pol. $F(x_1, \ldots, x_m)$ a coefficienti in $\mathbb{Z}$;

Generazione: Enumera, in maniera *esaustiva*—quanto meno in linea di principio—, le m-uple $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ di valori assegnabili alle variabili;

Valutazione: Per ogni m-upla, effettua la sostituzione $x_i \rightsquigarrow \boldsymbol{v}_i$ per $i = 1, \ldots, m$ e quindi calcola $F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$;

Test: Il valore trovato è 0? Emetti un responso positivo e fermati. (In caso contrario, la generazione va avanti).

Soluzione, ahimè illusoria, del X di Hilbert

Acquisizione dato: Il solito pol. $F(x_1, \ldots, x_m)$ a coefficienti in $\mathbb{Z}$;

Generazione: Enumera, in maniera *esaustiva*—quanto meno in linea di principio—, le m-uple $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ di valori assegnabili alle variabili;

Valutazione: Per ogni m-upla, effettua la sostituzione $x_i \rightsquigarrow \boldsymbol{v}_i$ per $i = 1, \ldots, m$ e quindi calcola $F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$;

Test: Il valore trovato è 0? Emetti un responso positivo e fermati. (In caso contrario, la generazione va avanti).

Esercizio: Delineare un modo sistematico di generare le m-uple.

lifelong obsession

"While I was still an undergraduate at City College in New York, I read my teacher E. L. Post's plaint that Hilbert's Tenth Problem

"begs for an unsolvability proof"

This was the beginning of my lifelong obsession with the problem." (*Martin Davis, 1993*)

(*Emil Leon Post, 1897–1954*)

Si può rispondere in modo negativo al X di Hilbert ?

" [$\cdots$] *ogni problema matematico, se precisato a dovere, dev'essere suscettibile di ricevere una composizione esatta: o nella forma di un'effettiva risposta alla domanda posta, o tramite la dimostrazione d'impossibilità di una sua soluzione e, conseguentemente, del necessario fallimento di ogni tentativo.* " [2]

" [$\cdots$] *every definite mathematical problem must necessarily be susceptible of an exact settlement, either in the form of an actual answer to the question asked, or by the proof of the impossibility of its solution and therewith the necessary failure of all attempts.* " [2]

Cosa è l'*Entscheidungsproblem* ?

assiomi $\alpha_1, \ldots, \alpha_n$ $\hookrightarrow$

congettura ϑ $\hookrightarrow$

$\boxed{\text{Decisore } \mathfrak{A}}$ $\hookrightarrow$ sí / no

Schema di un <u>ipotetico</u> risolutore per l'*Entscheidungsproblem*.

Cosa è l'*Entscheidungsproblem* ?

assiomi $\alpha_1, \ldots, \alpha_n$ $\hookrightarrow$

congettura ϑ $\hookrightarrow$

Decisore

$\mathfrak{A}$

$\hookrightarrow$ sí / no

Schema di un ipotetico risolutore per l'*Entscheidungsproblem*.
Il "sí" direbbe che una dimostrazione di ϑ esiste; il "no" che non esiste o addirittura che ϑ è *refutabile*

Cosa è l'*Entscheidungsproblem* ?

assiomi $\alpha_1, \ldots, \alpha_n$ $\hookrightarrow$
congettura ϑ $\hookrightarrow$

Decisore
$\mathfrak{A}$

$\hookrightarrow$ sí / no

Schema di un ipotetico risolutore per l'*Entscheidungsproblem*.
Il "sí" direbbe che una dimostrazione di ϑ esiste; il "no" che non esiste o addirittura che ϑ è *refutabile*, nel senso che dagli assiomi discende $\neg\vartheta$ anziché ϑ.

Cosa è l'*Entscheidungsproblem* ?

assiomi $\alpha_1, \ldots, \alpha_n$ $\hookrightarrow$ **Decisore** $\mathfrak{A}$ $\hookrightarrow$ sí / no

congettura ϑ $\hookrightarrow$

Schema di un ipotetico risolutore per l'*Entscheidungsproblem*.
Il "sí" direbbe che una dimostrazione di ϑ esiste; il "no" che non esiste o addirittura che ϑ è *refutabile*, nel senso che dagli assiomi discende $\neg\vartheta$ anziché ϑ. Da assiomi deboli potrebbe anche non discendere né ϑ né $\neg\vartheta$ e anche in questo caso la risposta del decisore sarebbe "no".

Che rapporto fra l'*Entscheidungsproblem* e il X problema ?

Che rapporto fra l'*Entscheidungsproblem* e il X problema ?

Andate a cercare gli assiomi di Peano...

Martin Davis.
One equation to rule them all.
Transactions of the New York Academy of Sciences. Series II, 30(6):766–773, 1968.

David Hilbert.
Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker-Kongreß zu Paris 1900.
Nachrichten von der Königliche Gesellschaft der Wissenschaften zu Göttingen, pages 253–297, 1900.

Thoralf Skolem.
Über die Nicht-charakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschliesslich Zahlenvariablen.
Fundamenta Mathematicae, 23:150–161, 1934.

Alfred Tarski.
A decision method for elementary algebra and geometry.
Technical Report R-109, RAND Corporation, Santa Monica, CA, 1948.
Prepared for publication with the assistance of J.C.C. McKinsey. Revised 1951, 2nd edition 1957.

Carl Ludwig Siegel.
Zur Theorie der quadratischen Formen.
Nachrichten der Akademie der Wissenschaften in Göttingen. II. Mathematisch-Physikalische Klasse, 3:21–46, 1972.

Martin Davis.
Hilbert's tenth problem is unsolvable.
Amer. Math. Monthly, 80(3):233–269, 1973.
Reprinted with corrections in the Dover edition of *Computability and Unsolvability* [9, pp. 199–235].

Yuri Vladimirovich Matiyasevich.
Hilbert's tenth problem.
The MIT Press, Cambridge (MA) and London, 1993.

Martin Davis.
Il decimo problema di Hilbert: equazioni e computabilità.
In Claudio Bartocci and Piergiorgio Odifreddi, editors, *La matematica – Pensare il mondo,* Volume IV, Grandi Opere.
Einaudi, 2010.

Martin Davis.
Computability and Unsolvability.
McGraw-Hill, New York, 1958.
Reprinted with an additional appendix, Dover 1983.

Un film documentario su Julia Robinson

"*Julia Robinson and Hilbert's Tenth Problem*" by George Csicsery is available from Zala Films, Oakland, California. See:

- `http://www.zalafilms.com/films/juliarobinson.html`
- `http://www.ams.org/ams/julia.html`