Insiemi 'definibili' tramite equazioni

Eugenio G. Omodeo

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Dip. Matematica e Geoscienze — DMI

Trieste, 30.03.2016

Sunto

A due linguaggi equazionali faremo corrispondere due famiglie di insiemi 'elencabili': gli insiemi

- *diofantei polinomiali* e quelli
- *diofantei esponenziali*. [1]

Indicando le tre famiglie con

$\mathfrak{D}$: diofantei polinomiali,
$\mathfrak{E}$: diofantei esponenziali,
$\mathfrak{R}$: elencabili,

risulterà chiaro che $\mathfrak{D} \subseteq \mathfrak{E} \subseteq \mathfrak{R}$.

[1] Questi concetti verranno riferiti non solo ai sottoinsiemi di $\mathbb{N}$ ma anche ai sottoinsiemi di potenze cartesiane finite $\mathbb{N}^n$ di $\mathbb{N}$.

Sunto

A due linguaggi equazionali faremo corrispondere due famiglie di insiemi 'elencabili': gli insiemi

- *diofantei polinomiali* e quelli
- *diofantei esponenziali*. [1]

Indicando le tre famiglie con

$\mathfrak{D}$: diofantei polinomiali,
$\mathfrak{E}$: diofantei esponenziali,
$\mathfrak{R}$: elencabili,

risulterà chiaro che $\mathfrak{D} \subseteq \mathfrak{E} \subseteq \mathfrak{R}$.

Si tratta di inclusioni strette o di uguaglianze ? ☞

[1] Questi concetti verranno riferiti non solo ai sottoinsiemi di $\mathbb{N}$ ma anche ai sottoinsiemi di potenze cartesiane finite $\mathbb{N}^n$ di $\mathbb{N}$.

Cenno su $\mathfrak{R}$

Chiamiamo ELENCO è una funzione computabile e iniettiva

- definita su tutto $\mathbb{N}$ o su di un intervallo $\{0, 1, \ldots, \ell - 1\}$ di naturali consecutivi;
- a valori in una potenza cartesiana $\mathbb{N}^n$.

L'insieme di tutte le immagini di un elenco si dice ELENCABILE.

Cenno su $\mathfrak{R}$

Chiamiamo ELENCO è una funzione computabile e iniettiva

- definita su tutto $\mathbb{N}$ o su di un intervallo $\{0, 1, \ldots, \ell - 1\}$ di naturali consecutivi;
- a valori in una potenza cartesiana $\mathbb{N}^n$.

L'insieme di tutte le immagini di un elenco si dice ELENCABILE.

N.B.: Vi sono $R \in \mathfrak{R}$ con il complementare $\overline{R} \notin \mathfrak{R}$

Anticipazione su $\mathfrak{D}$

Nella caratterizzazione di $\mathfrak{D}$ interverranno polinomi, specificabili nella forma

$$\sum_{\substack{0 \leqslant i_1 \leqslant n_1 \\ 0 \leqslant i_2 \leqslant n_2 \\ \vdots \\ 0 \leqslant i_k \leqslant n_k}} \lambda_{i_1, i_2, \ldots, i_k} \; y_1^{i_1} \cdots y_k^{i_k} \,,$$

dove

Anticipazione su $\mathfrak{D}$

Nella caratterizzazione di $\mathfrak{D}$ interverranno polinomi, specificabili nella forma

$$\sum_{\substack{0 \leqslant i_1 \leqslant n_1 \\ 0 \leqslant i_2 \leqslant n_2 \\ \vdots \\ 0 \leqslant i_k \leqslant n_k}} \lambda_{i_1, i_2, \ldots, i_k} \; y_1^{i_1} \cdots y_k^{i_k} \; ,$$

dove

- $k, n_1, \ldots, n_k$ sono numeri naturali,
- $y_1, \ldots, y_k$ sono variabili (suddivise in *incognite* e *parametri*),
- i numeri $\lambda_{i_1, i_2, \ldots, i_k}$ sono interi — *positivi, negativi, o zero*.

Anticipazione su $\mathfrak{E}$

Nella caratterizzazione di $\mathfrak{E}$ interverranno funzioni piú generali, specificabili nella forma

$$E_{sn}(\, y_1, \ldots, y_k \,) \quad - \quad E_{dx}(\, y_1, \ldots, y_k \,) \;,$$

dove E_{sn} ed E_{dx} sono espressioni costruite a partire da

- variabili y_h (suddivise c.s.) e da
- numeri naturali,
- tramite i costrutti $u + v$, $u\, v$, u^v di somma, prodotto ed *esponenziazione*.

Anticipazione su $\mathfrak{E}$

Nella caratterizzazione di $\mathfrak{E}$ interverranno funzioni piú generali, specificabili nella forma

$$E_{sn}(\, y_1, \ldots, y_k \,) \quad - \quad E_{dx}(\, y_1, \ldots, y_k \,) \;,$$

dove E_{sn} ed E_{dx} sono espressioni costruite a partire da

- variabili y_h (suddivise c.s.) e da
- numeri naturali,
- tramite i costrutti $u + v$, $u\, v$, u^v di somma, prodotto ed *esponenziazione*.

L'impiego estremamente limitato della sottrazione ci eviterà di doverci misurare con espressioni 'opache' quali la

$$(x - y)^{2^{2^{x-y}}}$$

(che valore dovrebbe assumere, questa, per $x = 2$ ed $y = 4$?)

Scaletta

Un classico: l'equazione di Mordell

Claude-Gaspard Bachet de Méziriac (1581–1638)

Louis Joel Mordell (1888–1972)

si appassionarono alla risoluzione dell'equazione

$$y^2 = x^3 + \kappa$$

(cosí pure Fermat, per $\underbrace{\kappa = -2 \text{ e } \kappa = -4}_{\text{risolubile}}$; Lebesgue per $\underbrace{\kappa = 7}_{\text{irresolubile}}$).

Un classico: l'equazione di Mordell

Claude-Gaspard Bachet de Méziriac (1581–1638)

Louis Joel Mordell (1888–1972)

si appassionarono alla risoluzione dell'equazione

$$y^2 = x^3 + \kappa$$

☜ param.

(cosí pure Fermat, per $\underbrace{\kappa = -2 \text{ e } \kappa = -4}_{\text{risolubile}}$; Lebesgue per $\underbrace{\kappa = 7}_{\text{irresolubile}}$).

Un classico: l'equazione di Mordell –II

Se $\kappa \neq 0$, il numero di soluzioni su $\mathbb{Z}$ è finito (Mordell, 1922); per quali κ càpita che manchino del tutto?

`http://oeis.org/A054504`
`http://oeis.org/A081121`

Un classico: l'equazione di Mordell –II

Se $\kappa \neq 0$, il numero di soluzioni su $\mathbb{Z}$ è finito (Mordell, 1922); per quali κ càpita che manchino del tutto?

`http://oeis.org/A054504`
`http://oeis.org/A081121`

E se eleggessimo a param. y invece di κ ?

$$\left.\begin{array}{rcl} y^2 & = & x^3 + \kappa \\ & \Downarrow & \\ y^2 & = & x^3 + \kappa \end{array}\right\} \text{banalizzaz.}$$

Altro classico: equazione di ब्रह्मगुप्त e le mandrie del Sole

Lagrange, ca. 1768: L'equazione 'di Pell'

$$x^2 - d\,y^2 \;=\; 1 \qquad \text{con} \quad d \in \mathbb{N} \setminus \{0\}$$

ha, su $\mathbb{N}$, sol. $\neq \langle 1, 0 \rangle$ se (e solo se) d *non* è un quadrato perfetto.

Altro classico: equazione di ब्रह्मगुप्त e le mandrie del Sole

Lagrange, ca. 1768: L'equazione 'di Pell'

$$x^2 - d\,y^2 \;=\; 1 \qquad \text{con} \quad d \in \mathbb{N} \setminus \{0\}$$

ha, su $\mathbb{N}$, sol. $\neq \langle 1, 0 \rangle$ se (e solo se) d *non* è un quadrato perfetto.

Pertanto la sua variante

$$x^2 - d\,(\,y + 1\,)^2 \;=\; 1$$

ha, su $\mathbb{N}$, soluzioni sse d *non* è un quadrato oppure $d = 0$.

Esempio piú classico che mai: le terne pitagoriche

"Numeri p.: sono le soluzioni intere dell'equazione p., per es.: 3, 4, 5; 5, 12, 13. La soluzione generale in numeri interi dell'equazione p., dovuta a Diofanto, è (salvo lo scambio di a con b):

$$a = x^2 - y^2\,; \qquad b = 2\,x\,y\,; \qquad c = x^2 + y^2\,,$$

con x, y interi ed $x > y$."

Dizionario Enciclopedico Italiano Treccani, 1970.

Esempio piú classico che mai: le terne pitagoriche

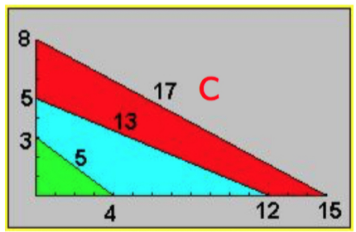
"Numeri p.: sono le soluzioni intere dell'equazione p., per es.: 3, 4, 5; 5, 12, 13. La soluzione generale in numeri interi dell'equazione p., dovuta a Diofanto, è (salvo lo scambio di a con b):

$$a = x^2 - y^2\,; \qquad b = 2\,x\,y\,; \qquad c = x^2 + y^2\,,$$

con x, y interi ed $x > y$."

Dizionario Enciclopedico Italiano Treccani, 1970.

Terne pitagoriche:



$$\begin{cases} a = x^2 - y^2 \\ b = 2\,x\,y \\ c = x^2 + y^2 \\ x = 1 + \bullet + y \\ y = 1 + \bullet \end{cases}$$

☜ $a^2 + b^2 = c^2$

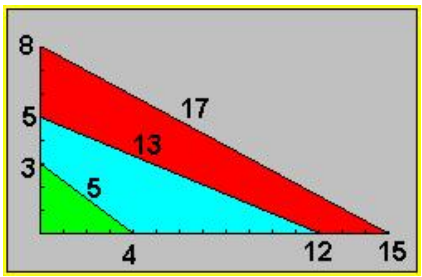
Esempio piú classico che mai: le terne pitagoriche

"Numeri p.: sono le soluzioni intere dell'equazione p., per es.: 3, 4, 5; 5, 12, 13. La soluzione generale in numeri interi dell'equazione p., dovuta a Diofanto, è (salvo lo scambio di a con b):

$$a = x^2 - y^2 ; \qquad b = 2xy ; \qquad c = x^2 + y^2 ,$$

con x, y interi ed $x > y$."

Dizionario Enciclopedico Italiano Treccani, 1970.



Come 'soluzione' di un'equazione parametrica, ci viene proposto un altro sistema *diofanteo su $\mathbb{N}$ nei* parametri *a, b, c e nelle* incognite*: x , y , piú altre due, implicite nel requisito $x > y > 0$.*

Capovolgimento di prospettiva

Quali insiemi, alla stessa stregua dell'insieme de

- le terne pitagoriche,
- i numeri non-quadrati,

sono *specificabili* ('definibili')
per mezzo di equaz. diofantee ?

Da questa prospettiva nasce
la pietra miliare, [Rob52], di

Julia Bowman Robinson (1919–1985)

Equazioni parametriche

Si consideri una funzione F in un numero finito k di argomenti,

$$F: \quad \mathbb{N}^k \longrightarrow \mathbf{S}, \quad \text{a valori in qualche} \quad \mathbf{S} \supseteq \mathbb{N}$$

(di solito, $\mathbf{S} = \mathbb{Z}$ oppure $\mathbf{S} = \mathbb{N} \cup \{\perp\}$).

l'‘indefinito’

Per quali valori $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ *dei* PARAMETRI *l'eq.*

$$F(\overbrace{\underbrace{a_1, \ldots, a_n}_{\text{parametri}}, \underbrace{x_1, \ldots, x_m}_{\text{incognite}}}^{k=n+m}) = 0$$

ha soluzione nelle INCOGNITE $x_1, \ldots, x_m$ *(su* $\mathbb{N}$ *) ?*

Salvo contrario avviso, le lettere latine minuscole spazieranno su $\mathbb{N}$.

Insiemi definibili (di dimensione n)

Si dice che un'equazione

$$F(\, a_1, \ldots, a_n \,, x_1, \ldots, x_m \,) \;=\; 0$$

DEFINISCE (esistenzialmente) l'insieme di tutte quelle n-uple $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \rangle$ di valori per le quali essa è risolubile.

Insiemi definibili (di dimensione n)

Si dice che un'equazione

$$F(\, a_1, \ldots, a_n \,, x_1, \ldots, x_m \,) \;=\; 0$$

DEFINISCE (esistenzialmente) l'insieme di tutte quelle n-uple $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \rangle$ di valori per le quali essa è risolubile.

Di una *proprietà*, *relazione*, *funzione* (anche solo parziale) su $\mathbb{N}$, ci domanderemo:

"*è definibile mediante una funzione di un certo tipo ?*" [2]

Per $n = 0$,

[2] Qui entrano in campo $\mathfrak{D}$ ed $\mathfrak{E}$.

Insiemi definibili (di dimensione n)

Si dice che un'equazione

$$F(\, a_1, \ldots, a_n \,, x_1, \ldots, x_m \,) \;=\; 0$$

DEFINISCE (esistenzialmente) l'insieme di tutte quelle n-uple $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \rangle$ di valori per le quali essa è risolubile.

Di una *proprietà*, *relazione*, *funzione* (anche solo parziale) su $\mathbb{N}$, ci domanderemo:

"*è definibile mediante una funzione di un certo tipo ?*" [2]

Per $n = 0$, la questione torna a essere quella classica (hilbertiana):
"*esistono, o no, soluzioni ?*"

[2] Qui entrano in campo $\mathfrak{D}$ ed $\mathfrak{E}$.

Un esempio di dimensione $n = 1$

$a = (2x + 3)y$ definisce .....

Un esempio di dimensione $n = 1$

$a = (2x + 3)y$ definisce $\mathbb{N} \setminus \{\text{potenze di } 2\}$

Una schiera $\mathcal{B}_k(a_0, a_1)$ di relaz. definibili senza incognite

Per ogni $k \in \mathbb{N}$, la rel. diadica

$$a_0 \quad = \quad \sum_{i=0}^{a_1} i^k$$

è definita da un'eq.

$$a_0 - B(a_1) \quad = \quad 0 \quad ,$$

dove $B \in \mathbb{Q}[a_1] = 0$ ha grado $k+1$. (Jakob Bernoulli, XVII sec.)

(Ada Lovelace all'opera nel 1843)

Di nuovo un esempio di dimensione $n = 1$

$$a = x^2 + v^2 + y^2 + z^2 \qquad \text{definisce} \quad \mathbb{N}$$

$$a = x^2 + x + y^2 + z^2 \qquad \text{definisce} \quad \mathbb{N}$$

(Joseph-Louis Lagrange, ca. 1770)

(Adrien-Marie Legendre, 1798)

Di nuovo un esempio di dimensione $n = 1$

$a = x^2 + v^2 + y^2 + z^2$ definisce $\mathbb{N}$

$a = x^2 + x + y^2 + z^2$ definisce $\mathbb{N}$

(Joseph-Louis Lagrange, ca. 1770)

(Adrien-Marie Legendre, 1798)

$a - x = 0$ definisce $\mathbb{N}$

Un esempio di dimensione $n = 4$

Definizione *polinomiale* dell'appaiata di QUOZIENTE e RESTO su $\mathbb{N}$:

$$a = c \div d \;\&\; b = c \,\%\, d$$

$$\Downarrow$$

$$a\,d + b = c \;\&\; b < d$$

$$\Downarrow$$

$$(a\,d + b - c)^2 + (b + x + 1 - d)^2 = 0$$

Esempio: proiezioni di polinomi iniettivi

Nel 1971, Nikolaj Kirillovič Kosovskiĭ propose il polinomio

$$\kappa_m(\, x_1\, , \ldots ,\, x_m\,) \quad =_{\mathsf{Def}} \quad \sum_{i=1}^{m} \left(\sum_{j=1}^{i} x_j \right)^i$$

per codificare, le m-uple su $\mathbb{N}$, per ciascun m.

Esempio: proiezioni di polinomi iniettivi

Nel 1971, Nikolaj Kirillovič Kosovskiĭ propose il polinomio

$$\kappa_m(\, x_1\, ,\ldots,\, x_m\,) \quad =_{\mathrm{Def}} \quad \sum_{i=1}^{m} \left(\sum_{j=1}^{i} x_j\right)^i$$

per codificare, le m-uple su $\mathbb{N}$, per ciascun m.

Teorema. Non vi sono, per alcun m, due m-uple $\langle x_1, \ldots, x_m\rangle$, $\langle y_1, \ldots, y_m\rangle$ a componenti in $\mathbb{N}$ tali che

$$\kappa_m(\, x_1\, ,\ldots,\, x_m\,) \quad = \quad \kappa_m(\, y_1\, ,\ldots,\, y_m\,) \quad .$$

Esempio: proiezioni di polinomi iniettivi

Nel 1971, Nikolaj Kirillovič Kosovskiĭ propose il polinomio

$$\kappa_m(x_1 , \ldots , x_m) \quad =_{\text{Def}} \quad \sum_{i=1}^{m} \left(\sum_{j=1}^{i} x_j \right)^i$$

per codificare, le m-uple su $\mathbb{N}$, per ciascun m.

Teorema. Non vi sono, per alcun m, due m-uple $\langle x_1, \ldots, x_m \rangle$, $\langle y_1, \ldots, y_m \rangle$ a componenti in $\mathbb{N}$ tali che

$$\kappa_m(x_1 , \ldots , x_m) \quad = \quad \kappa_m(y_1 , \ldots , y_m) \quad .$$

Ciascuna

$$a \quad = \quad \pi_i^m(b)$$

delle proiezioni di un κ_m è definibile polinomialmente:

$$b \quad = \quad \kappa_m(x_1 , \ldots , x_{i-1} , a , x_{i+1} , \ldots , x_m) \quad .$$

Qualche altro esempio di dimensione $n = 1$

$a = (x+2)(y+2)$ definisce .....

$x^2 - a(y+1)^2 = 1$ definisce $\{0\} \cup (\mathbb{N} \setminus \{\text{quadrati perfetti}\})$

(Brahmagupta, 628 $\Rrightarrow$ Joseph L. Lagrange, 1768)

$(a+1)(a-m_1)\cdots(a-m_h) = (x+1)$

Qualsiasi sottoinsieme cofinito di $\mathbb{N}$ è definibile tramite polinomio

Qualche altro esempio di dimensione $n = 1$

$a = (x+2)(y+2)$ definisce l'insieme dei *numeri composti*

$x^2 - a(y+1)^2 = 1$ definisce $\{0\} \cup (\mathbb{N} \setminus \{\text{quadrati perfetti}\})$

(Brahmagupta, 628 $\Rightarrow$ Joseph L. Lagrange, 1768)

$(a+1)(a-m_1)\cdots(a-m_h) = (x+1)$

Qualsiasi sottoinsieme cofinito di $\mathbb{N}$ è definibile tramite polinomio

Qualche altro esempio di dimensione $n = 1$

$a = (x+2)(y+2)$ definisce l'insieme dei *numeri composti*

$x^2 - a(y+1)^2 = 1$ definisce $\{0\} \cup (\mathbb{N} \setminus \{\text{quadrati perfetti}\})$

(Brahmagupta, 628 $\Rrightarrow$ Joseph L. Lagrange, 1768)

$(a+1)(a-m_1)\cdots(a-m_h) = (x+1)$

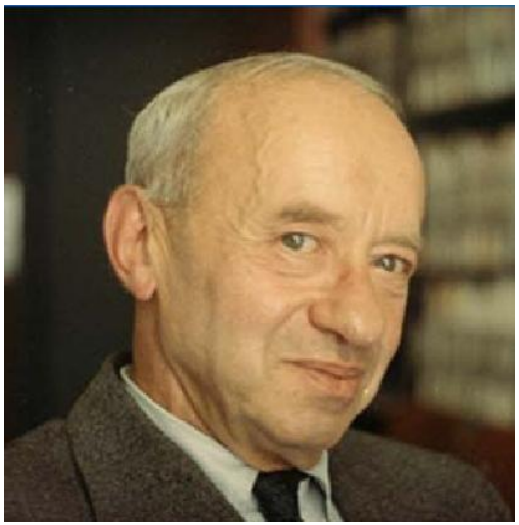
Qualsiasi sottoinsieme cofinito di $\mathbb{N}$ è definibile tramite polinomio

$(x+1)^a + (y+1)^a = (z+1)^a$ definisce l'insieme $\{1,2\}$

(Pierre de Fermat, 1637 $\Rrightarrow$ Andrew J. Wiles, 1994)

Non definibile polinomialmente ?

"*A towering figure in mathematics and logic*".



Alfred Tarski, nato Tajtelbaum (1901–1983)

Negli anni 1940, Tarski si aspetta che

$$\{\, 2^h : h \in \mathbb{N} \,\} \notin \mathfrak{D}$$

$$\therefore \mathfrak{E} \neq \mathfrak{D}$$

Un'ipotesi piuttosto contro-intuitiva

Julia Bowman Robinson (1919–1985)

Ca. 1950, J. Robinson

cerca di dimostrare che

$$\left\{\langle a, b, c\rangle \,:\, a^b = c\right\} \in \mathfrak{D}$$
$$\therefore \mathfrak{D} = \mathfrak{E}$$

Su quale 'evidenza' poggiava la congettura J.R. ?

Soluzioni dell'equazione di Pell (Un'intuiz. *serendipitous*)

Consideriamo le soluzioni su $\mathbb{N}$ dell'eq.

$$X^2 - (\underbrace{a^2 - 1}_{d})\, Y^2 \;=\; 1\,, \quad \text{con} \quad a \geqslant 2\,.$$

Si tratta di tutte sole le coppie

$$X = \boldsymbol{x}_a(b)\,, \quad Y = \boldsymbol{y}_a(b)\,, \qquad \text{con} \quad b \in \mathbb{N}\,, \qquad \text{tali che}$$

$$\boldsymbol{x}_a(b) + \boldsymbol{y}_a(b)\sqrt{d} \;=\; \left(a + \sqrt{d}\,\right)^b .$$

Questi numeri irrazionali crescono grosso modo come a^b !

Relazioni a crescita esponenziale

Si dice che una relazione $\mathcal{J} \subseteq \mathbb{N} \times \mathbb{N}$ è A CRESCITA ESPONENZIALE quando soddisfa le seguenti due condizioni:

- $\mathcal{J}(u, v)$ implica che $v < u^u$, per ogni u e ogni v;
- per ogni k, ci sono numeri u, v per i quali $\mathcal{J}(u, v)$ ed $u^k < v$.

Vi sono relazioni di questa natura che siano diofantee polinomiali ?

Relazioni a crescita esponenziale

Si dice che una relazione $\mathcal{J} \subseteq \mathbb{N} \times \mathbb{N}$ è A CRESCITA ESPONENZIALE quando soddisfa le seguenti due condizioni:

- $\mathcal{J}(u, v)$ implica che $v < u^u$, per ogni u e ogni v;
- per ogni k, ci sono numeri u, v per i quali $\mathcal{J}(u, v)$ ed $u^k < v$.

Vi sono relazioni di questa natura che siano diofantee polinomiali ?
In [Rob52]

- J.R. ipotizza di sí;
- mostra che se ce n'è almeno una, allora $\mathfrak{D} = \mathfrak{E}$;
- trova plausibile che vi sia un insieme $D \in \mathfrak{D}$ con complementare $\overline{D} \notin \mathfrak{R}$

Relazioni a crescita esponenziale

Si dice che una relazione $\mathcal{J} \subseteq \mathbb{N} \times \mathbb{N}$ è A CRESCITA ESPONENZIALE quando soddisfa le seguenti due condizioni:

- $\mathcal{J}(u, v)$ implica che $v < u^u$, per ogni u e ogni v;
- per ogni k, ci sono numeri u, v per i quali $\mathcal{J}(u, v)$ ed $u^k < v$.

Vi sono relazioni di questa natura che siano diofantee polinomiali ?
In [Rob52]

- J.R. ipotizza di sí;
- mostra che se ce n'è almeno una, allora $\mathfrak{D} = \mathfrak{E}$;
- trova plausibile che vi sia un insieme $D \in \mathfrak{D}$ con complementare $\overline{D} \notin \mathfrak{R}$

(∴ insolubile il X problema di Hilbert).

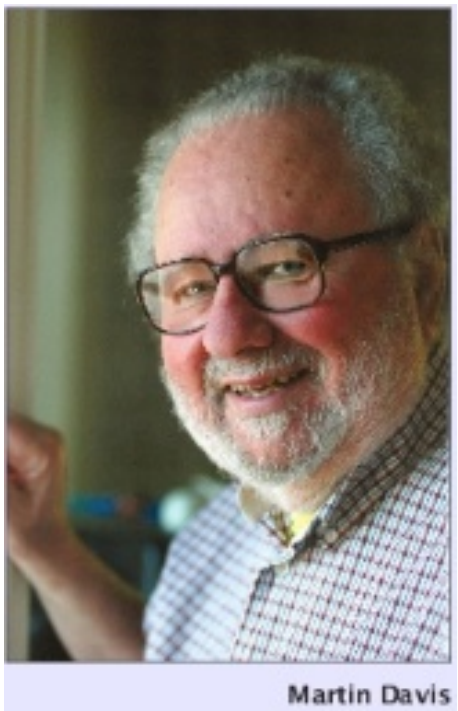
Un'ipotesi ancor piú audace

"*Martin Davis [1953] set forth the daring hypothesis that* [· · ·] every semidecidable set is Diophantine."

[Mat93, p. 99]

Su quale 'evidenza' poggiava tale congettura ?

Altra intuizione *serendipitous*


Martin Davis

Martin D. Davis (1928 –)

Ca. 1950, M. Davis:

- nota che $\mathfrak{D}$ è chiusa rispetto a $\cup$ ed $\cap$
- trova una dim. non-costruttiva che $\mathfrak{D}$ *non* è chiusa rispetto alla complementazione.

Qui risiede un'analogia con $\mathfrak{R}$

I numeri del triangolo di Tartaglia

Per una specifica esponenziale di

$$\langle b, c\rangle \longmapsto \binom{b}{c} = \textit{numero delle combinazioni di } b \textit{ oggetti presi a gruppi di } c\,,$$

osserviamo che se $u > 2^b$,

I numeri del triangolo di Tartaglia

Per una specifica esponenziale di

$$\langle b, c \rangle \longmapsto \binom{b}{c} = \begin{array}{l} \textit{numero delle combinazioni di} \\ b \textit{ oggetti presi a gruppi di } c \textit{ ,} \end{array}$$

osserviamo che se $u > 2^b$, allora

- $u > \binom{b}{k}$ per $k = 0, 1, \ldots, b$ (e oltre) ;
- $(u+1)^b = \sum_{k=0}^{b} \binom{b}{k} u^k$.

Per estrarre di qui la 'cifra' $a = \binom{b}{c}$, riferita alla base u, usiamo *quoziente* e *resto*:

$$a = \left(\left((u+1)^b \div u^c\right) \,\%\, u\right) \quad \wedge \quad u = 2^b + 1 \ .$$

Una variante generalizzata della progressione geometrica

Yuri V. Matiyasevich [Mat93, pagg. 202 e 203] ci dimostra che è diofantea esponenziale a relazione triadica

$$\left\{ \left\langle \sum_{i=0}^{a} b^i \, i^k, \; a, \; b \right\rangle : a \in \mathbb{N}, \; b \in \mathbb{N} \right\},$$

per ogni $k \in \mathbb{N}$.

Da un teorema del 1878 a una specifica della dominanza

Scriviamo che

$$a \sqsubseteq b \qquad (\text{ '}b \text{ DOMINA } a\text{' }) \ ,$$

se, scritti tali numeri come

$$a = \sum_{i=0}^{k} a_i \, 2^i \ , \qquad b = \sum_{i=0}^{k} b_i \, 2^i \ , \qquad \textit{con}$$

$$a_i, b_i \in \{0,1\} \qquad \textit{per} \quad i = 0, 1, \ldots, k \ ,$$

fra i loro bit intercorrono le relaz.

$$a_i \leqslant b_i \qquad \textit{per} \quad i = 0, 1, \ldots, k \ .$$

La specifica diofantea esponenziale che fa al caso nostro è:

$$2\,x + 1 = \left(\left((u+1)^b \div u^a\right) \,\%\, u\right) \quad \wedge \quad u = 2^b + 1 \ .$$

Specifica esponenziale del fattoriale

Lemma. (Julia Robinson) Vale

$$j! \leqslant \frac{r^j}{\binom{r}{j}} < j! + 1 \qquad \text{quando} \quad r > (2\,j)^{j+1}$$

Corollario.

$$m = j! \quad \textbf{sse} \quad m = \left((2j+1)^{2j+1}\right)^j \div \binom{(2j+1)^{2j+1}}{j}$$

Semplificazione. (Yuri Vladimirovich Matiyasevich)

$$m = j! \quad \textbf{sse} \quad m = \left((j+2)^{j+2}\right)^j \div \binom{(j+2)^{j+2}}{j}$$

Coprimalità e primalità

Indichiamo con $a \perp b$ la *coprimalità* fra a e b. Allora:

$$a \perp b \quad \textbf{sse} \quad (\exists\, \chi, \eta \in \mathbb{Z} \mid \chi\, a + \eta\, b = 1)$$

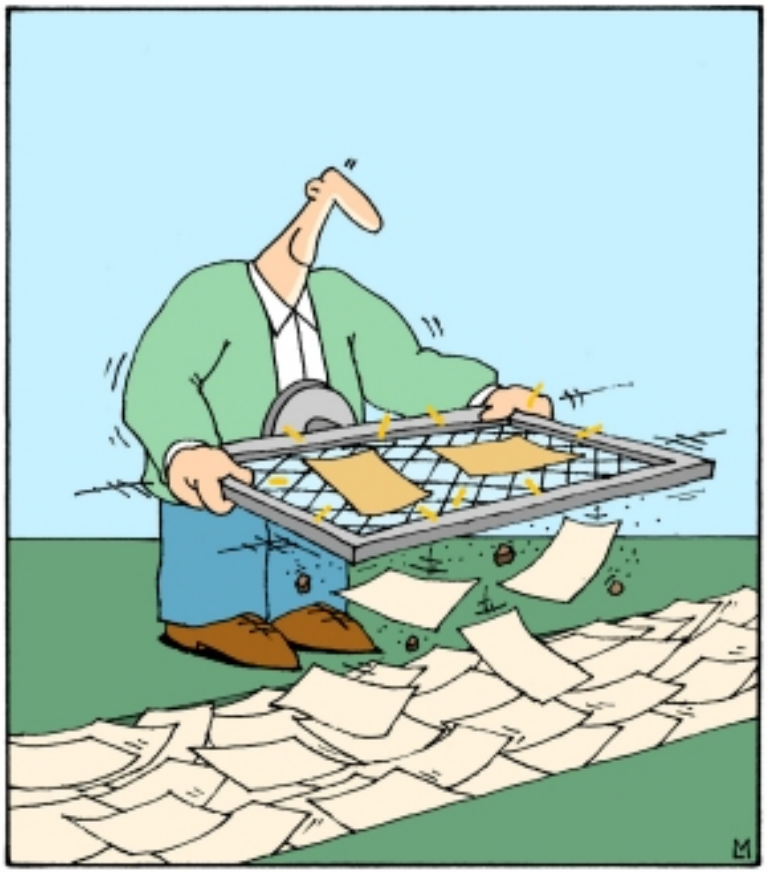
Una specifica diofantea polinomiale di $a \perp b$ è:

$$(x_1 - x_2)\, a + (y_1 - y_2)\, b \;=\; 1$$

Una specifica diofantea esponenziale della *primalità* è:

$$\text{Primo}(\, a \,) \quad \textbf{sse} \quad a > 1 \;\wedge\; (a-1)! \perp a$$

Voci bibliografiche




Martin Davis.
Hilbert's tenth problem is unsolvable.
The American Mathematical Monthly, 80(3):233–269, 1973.


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.


James P. Jones, Daihachiro Sato, Hideo Wada, and Douglas Wiens.
Diophantine representation of the set of prime numbers.
American Mathematical Monthly, 83(6):449–464, 1976.


Yuri Ivanovich Manin.
A course in mathematical logic.
Graduate texts in Mathematics. Springer-Verlag, 1977.


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


Julia Robinson.
Existential definability in arithmetic.
Transactions of the American Mathematical Society, 72(3):437–449, 1952.