Julia Robinson e il 10º problema di Hilbert

natural numbers. To me they are the one real thing. We can conceive of a chemistry which is different from ours, or a biology, but we cannot conceive of a different mathematics of numbers. What is proved about numbers will be a fact in any universe.

(J.R.)

Eugenio G. Omodeo, Trieste, 23.03.2021

Indice dei contenuti

[1] La piccola immagine di Julia Robinson nel frontespizio è stata creata da Massimo Franceschet

Il 10º problema di Hilbert (1900)

Un'equazione diofantea

$D(x_1, \ldots, x_m) = 0$ $\hookrightarrow$ 

$\hookrightarrow$ **sí / no**

Schema di un *ipotetico* risolutore per il 10º problema. Il responso:

Il 10º problema di Hilbert (1900)

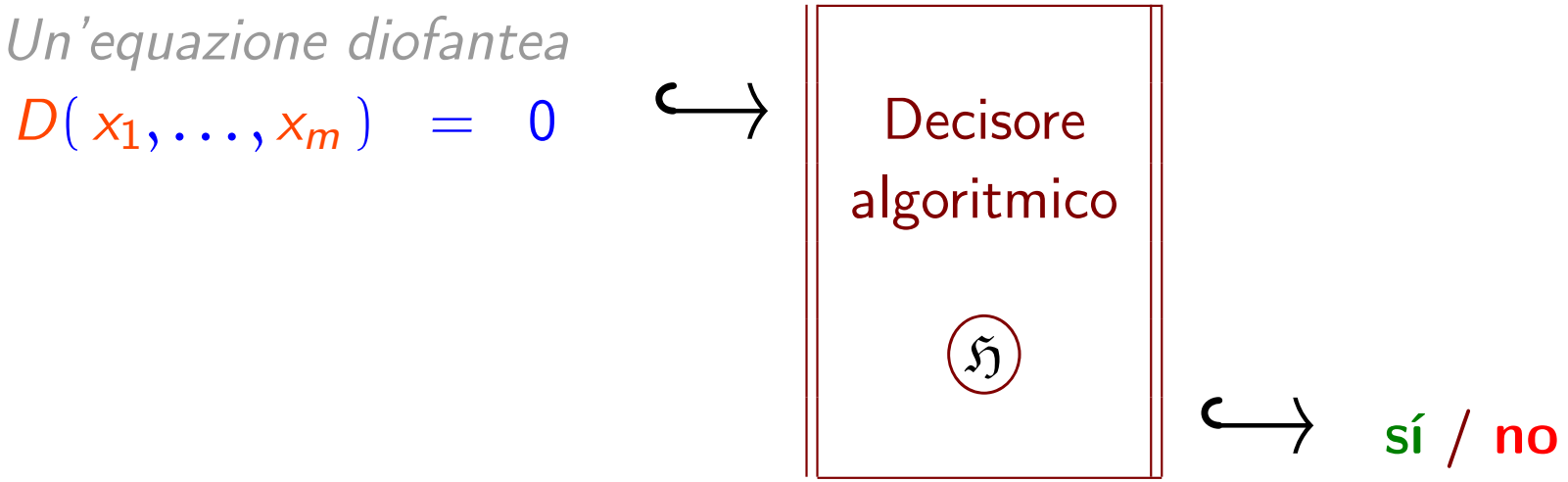
Un'equazione diofantea

$D(x_1, \ldots, x_m) = 0$ $\hookrightarrow$ 

$\hookrightarrow$ **sí** / **no**

Schema di un *ipotetico* risolutore per il 10º problema. Il responso: "**no**" indicherebbe che non vi sono soluzioni;

Il 10º problema di Hilbert (1900)



Schema di un *ipotetico* risolutore per il 10º problema. Il responso:

"**sí**" indicherebbe che c'è *almeno una* soluzione

$$\begin{cases} x_1 = v_1 \\ \vdots \quad \vdots \quad \vdots \\ x_m = v_m \end{cases}$$

dove ogni v_i è un intero (positivo, negativo, o nullo).

Che tipo di espressione è la $D(x_1, \ldots, x_m)$?

L'espressione D che vogliamo rendere uguale a 0 è costruita a partire da

- *costanti* intere (ad es. 8 , -2 , $100\,003$);
- *incognite* x_i ;

tramite i costrutti $+$ ed $\cdot$ di *somma* e *moltiplicazione*.

In altre parole D designa un **polinomio**

(multivariato e di grado qualsiasi).

Che tipo di espressione è la $D(x_1, \ldots, x_m)$?

L'espressione D che vogliamo rendere uguale a 0 è costruita a partire da

- *costanti* intere (ad es. 8 , -2 , $100\,003$);
- *incognite* x_i ;

tramite i costrutti $+$ ed $\cdot$ di *somma* e *moltiplicazione*.

In altre parole D designa un **polinomio**

(multivariato e di grado qualsiasi).

Osservazione:

$$P = 0 \vee Q = 0 \quad \rightsquigarrow \quad P \cdot Q = 0$$

$$P = 0 \,\&\, Q = 0 \quad \rightsquigarrow \quad P^2 + Q^2 = 0$$

Quale dei due sistemi di equazioni,

$$\begin{cases} 6\,W + 2\,X^2 - Y^3 &= 0 \\ 5\,X\,Y - Z^2 - 1 &= 0 \\ W^2 - W + 2\,X - Y + Z - 3 &= 0 \end{cases}$$

$$\begin{cases} 6\,W + 2\,X^2 - Y^3 &= 0 \\ 5\,X\,Y - Z^2 - 1 &= 0 \\ W^2 - W + 2\,X - Y + Z - 4 &= 0\,, \end{cases}$$

ammette soluzione *negli interi* e quale no? Argomentare la risposta.

Quale dei due sistemi di equazioni,

$$\begin{cases} 6\,W + 2\,X^2 - Y^3 &= 0 \\ 5\,X\,Y - Z^2 - 1 &= 0 \\ W^2 - W + 2\,X - Y + Z - 3 &= 0 \end{cases}$$

$$\begin{cases} 6\,W + 2\,X^2 - Y^3 &= 0 \\ 5\,X\,Y - Z^2 - 1 &= 0 \\ W^2 - W + 2\,X - Y + Z - 4 &= 0\,, \end{cases}$$

ammette soluzione *negli interi* e quale no? Argomentare la risposta.

Lo 'spazio' ove cercare l'attestazione non è lo stesso nei due casi !

Esempio: 100 istanze risolte del $10^{\underline{o}}$ di H.

Per quali interi $\kappa > 0$ è risolubile l'equazione $x^3 + y^3 + z^3 = \kappa$?

L'ultima tassello mancante, per $\kappa \leqslant 100$, rimaneva $\kappa = 42$.
Clicca qui!! È andato a posto nell'autunno 2019:

$$\begin{aligned} &-80,538,738,812,075,974^3 \\ &+80,435,758,145,817,515^3 \\ &+12,602,123,297,335,631^3 \quad = \quad 42 \end{aligned}$$

2019

1	2	3	~~X~~	~~X~~	6	7	8	9	10
11	12	~~X~~	~~X~~	15	16	17	18	19	20
21	~~X~~	~~X~~	24	25	26	27	28	29	30
~~X~~	~~X~~	33	34	35	36	37	38	39	~~X~~
~~X~~	42	43	44	45	46	47	48	~~X~~	~~X~~
51	52	53	54	55	56	57	~~X~~	~~X~~	60
61	62	63	64	65	66	~~X~~	~~X~~	69	70
71	72	73	74	75	~~X~~	~~X~~	78	79	80
81	82	83	84	~~X~~	~~X~~	87	88	89	90
91	92	93	~~X~~	~~X~~	96	97	98	99	100

Di qui in poi lavoreremo in $\mathbb{N}$: ☞

J. Robinson si aspetta che il 10º sia insolubile

"Per molte classiche equazioni diofantee con un parametro non è noto un metodo effettivo che, comunque venga fissato il parametro, dica se l'equazione ha soluzioni o no; perciò è poco plausibile che si possa trovare un procedimento di decisione. Ad esempio, non si conoscono metodi che determinino per quali valori di a il sistema diofanteo

$$x^2 + a\,y^2 = s^2\,, \qquad x^2 - a\,y^2 = t^2$$

è risolubile. (Primi a studiare questo problema furono gli Arabi, nel Medio Evo)."

(J.R, 1952)

(Julia Bowman Robinson, 1919–1985)

Relazioni diofantee, esistenzialmente definibili, elencabili

Una relazione $\mathcal{D} \subseteq \mathbb{N}^{m}$ si dice ***definibile esistenzialm. in termini di una relazione*** $\mathcal{J}(\bullet, \ldots, \bullet)$ sse

$$\mathcal{D}(a_1, \ldots, a_m) \iff \exists x_1 \cdots \exists x_k \quad \varphi(\overbrace{a_1, \ldots, a_m}, \overbrace{x_1, \ldots, x_k})$$

vale, in $\mathbb{N}$, per qualche formula φ involgente solo :

Una relazione $\mathcal{D} \subseteq \mathbb{N}^{m}$ si dice ***definibile esistenzialm. in termini di una relazione*** $\mathcal{J}(\bullet, \ldots, \bullet)$ sse

$$\mathcal{D}(a_1, \ldots, a_m) \iff \exists\, x_1 \cdots \exists\, x_k \quad \varphi(\overbrace{\underbrace{a_1, \ldots, a_m}_{\text{parametri}}, \underbrace{x_1, \ldots, x_k}_{\text{incognite}}}^{\text{variabili distinte}})$$

vale, in $\mathbb{N}$, per qualche formula φ involgente solo :

- variabili individuali, quelle mostrate,
- costanti intere *positive*,

Una relazione $\mathcal{D} \subseteq \mathbb{N}^{m}$ si dice ***definibile esistenzialm. in termini di una relazione*** $\mathcal{J}(\bullet, \ldots, \bullet)$ sse

$$\mathcal{D}(a_1, \ldots, a_m) \iff \exists x_1 \cdots \exists x_k \quad \varphi(\overbrace{\underbrace{a_1, \ldots, a_m}_{\text{parametri}}, \underbrace{x_1, \ldots, x_k}_{\text{incognite}}}^{\text{variabili distinte}})$$

vale, in $\mathbb{N}$, per qualche formula φ involgente solo :

- operatori di addizione e moltiplicazione,
- i connettivi logici $=$, $\&$, $\vee$ ~~, $\neg$, $\forall$~~

Una relazione $\mathcal{D} \subseteq \mathbb{N}^{m}$ si dice ***definibile esistenzialm. in termini di una relazione*** $\mathcal{J}(\bullet, \ldots, \bullet)$ sse

$$\mathcal{D}(a_1, \ldots, a_m) \iff \exists x_1 \cdots \exists x_k \quad \varphi(\overbrace{a_1, \ldots, a_m}^{\text{parametri}}, \overbrace{x_1, \ldots, x_k}^{\text{incognite}})$$

variabili distinte

vale, in $\mathbb{N}$, per qualche formula φ involgente solo :

- variabili individuali, (come libere) quelle mostrate,
- costanti intere *positive*,
- operatori di addizione e moltiplicazione,
- i connettivi logici $=$, $\&$, $\vee$, $\exists \upsilon$, ed
- un predicato per $\mathcal{J}$.

Una relazione $\mathcal{D} \subseteq \mathbb{N}^{m}$ si dice ***definibile esistenzialm. in termini di una relazione*** $\mathcal{J}(\bullet, \ldots, \bullet)$ sse

$$\mathcal{D}(a_1, \ldots, a_m) \iff \exists x_1 \cdots \exists x_k \quad \varphi(\overbrace{a_1, \ldots, a_m}^{\text{parametri}}, \overbrace{x_1, \ldots, x_k}^{\text{incognite}})$$

variabili distinte

vale, in $\mathbb{N}$, per qualche formula φ involgente solo :

- variabili individuali, quelle mostrate,
- costanti intere *positive*,
- operatori di addizione e moltiplicazione,
- i connettivi logici $=$, $\&$, $\vee$, $\exists \upsilon$, ed
- un predicato per $\mathcal{J}$.

Quando $\mathcal{J}(\mathfrak{b}, \mathfrak{n}, \mathfrak{c})$ è $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$, $\mathcal{D}$ vien detta ***diofantea*** **esponenziale**.

Relazioni e proprietà diofantee *lato sensu*

Una relazione $\mathcal{D} \subseteq \mathbb{N}^{m}$ si dice ***definibile esistenzialm. in termini di una relazione*** $\mathcal{J}(\bullet, \ldots, \bullet)$ sse

$$\mathcal{D}(a_1, \ldots, a_m) \iff \exists\, x_1 \cdots \exists\, x_k \quad \varphi(\overbrace{a_1, \ldots, a_m}^{\text{parametri}}, \overbrace{x_1, \ldots, x_k}^{\text{incognite}})$$

variabili distinte

vale, in $\mathbb{N}$, per qualche formula φ involgente solo :

- variabili individuali, quelle mostrate,
- costanti intere *positive*,
- operatori di addizione e moltiplicazione,
- i connettivi logici $=$, $\&$, $\vee$, $\exists \mathfrak{v}$, ed
- un predicato per $\mathcal{J}$.

Quando $\mathcal{J}(\mathfrak{b}, \mathfrak{n}, \mathfrak{c})$ è $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$, $\mathcal{D}$ vien detta ***diofantea* esponenziale**.

Quando $\mathcal{J}$ non figura in φ, $\mathcal{D}$ vien detta ***diofantea***.

Una relazione $\mathcal{D} \subseteq \mathbb{N}^{m}$ si dice ***definibile esistenzialm. in termini di una relazione*** $\mathcal{J}(\bullet, \ldots, \bullet)$ sse

$$\mathcal{D}(a_1, \ldots, a_m) \iff \exists\, x_1 \cdots \exists\, x_k \quad \varphi(\overbrace{a_1, \ldots, a_m}^{\text{parametri}}, \overbrace{x_1, \ldots, x_k}^{\text{incognite}})$$

variabili distinte

vale, in $\mathbb{N}$, per qualche formula φ involgente solo :

- variabili individuali, quelle mostrate,
- costanti intere *positive*,
- operatori di addizione e moltiplicazione,
- i connettivi logici $=$, $\&$, $\vee$, $\exists \mathfrak{v}$, ed
- un predicato per $\mathcal{J}$.

Quando $\mathcal{J}(\mathfrak{b}, \mathfrak{n}, \mathfrak{c})$ è $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$, $\mathcal{D}$ vien detta ***diofantea* esponenziale**.

Quando $\mathcal{J}$ non figura in φ, $\mathcal{D}$ vien detta ***diofantea***.

Esempio balocco

- $(a+1)\cdot(a+1) = 1$,
- $a^a = 1 \quad \& \quad x^x = a+1$

definiscono esistenzialm. . . . *in termini di* ***esponenziazione*** $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$.

1

Esempio balocco

Entrambi

- $(a+1)\cdot(a+1) = 1$,
- $a^a = 1 \quad \& \quad x^x = a+1$

definiscono esistenzialm. $\{0\}$ *in termini di* ***esponenziazione*** $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$.

1

Entrambi

- $(a+1)\cdot(a+1) = 1$,
- $a^a = 1 \quad \& \quad x^x = a+1$

definiscono esistenzialm. $\{0\}$ *in termini di* ***esponenziazione*** $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$.

Come 0, molti altri utili costrutti diofantei, e.g.[1]

$$\bullet > \bullet, \quad \bullet \leqslant \bullet, \quad \bullet \nmid \bullet, \quad \bullet = \square, \quad \lfloor \bullet / \bullet \rfloor, \quad \bullet \,\%\, \bullet,$$

possono venir aggiunti al linguaggio delle definizioni esistenziali.

1

Come 0, molti altri utili costrutti diofantei, e.g.

$$\bullet > \bullet, \quad \bullet \leqslant \bullet, \quad \bullet \nmid \bullet, \quad \bullet = \square, \quad \lfloor \bullet / \bullet \rfloor, \quad \bullet \,\%\, \bullet,$$

possono venir aggiunti al linguaggio delle definizioni esistenziali.

---

[1] E.g.,

$$a \nmid b \iff \exists\, q\, \exists\, r\, \exists\, d\, \left(q \cdot a + \overbrace{r + 1}^{\textit{resto}} = b \;\&\; r + 1 + d + 1 = a \right).$$

Specifica diofantea di proprietà e relazioni

Esercizi: Esprimere tramite equazione diofantea parametrica:

1. $a \in \{4, 5, 9\}$
2. a dista 3 da b
3. $a \neq b$
4. $a \in \{0, 3, 6, \ldots, 30\}$
5. Fra i divisori di a c'è un quadrato perfetto
6. a è un numero dispari
7. a non è un divisore di b
8. a, b, c non è una terna pitagorica
9. a è un numero *composto* (cioè $a \neq 0$, $a \neq 1$ ed a non è un primo)
10. a *non* è una potenza del 2
11. a è un num. triangolare, cioè della forma $1 + 2 + \cdots + x$ per qualche num. naturale x
12. $a \geqslant MP2(b)$, dove $MP2(b)$ esprime la massima potenza del 2 che divide b (ad es.: $MP2(5) = 1$, $MP2(12) = 4$)
13. $a > 0$ e inoltre l'equazione $$a X^2 + b X + c = 0$$ con X incognita *complessa* ha soluzioni *razionali*.
14. c è il piú grande fra a e b

Vero che $a - \left(x^2 + x + 41\right) = 0$ rappresenta un insieme di primi consecutivi ?

Definizione (famiglia $\mathfrak{R}$ delle relazioni *elencabili*)

Si dice che una relazione $\mathcal{R} \subseteq \mathbb{N}^{\boldsymbol{m}}$ è ***elencabile*** se $\mathcal{R} = \emptyset$ oppure c'è una $\boldsymbol{m}$-upla $\langle h_1, \ldots, h_{\boldsymbol{m}} \rangle$ di funzioni

$$h : \ \mathbb{N} \longrightarrow \mathbb{N}$$

ricorsive primitive tale che

$$\mathcal{R}(a_1, \ldots, a_{\boldsymbol{m}}) \iff \exists\, i \in \mathbb{N} \quad \langle a_1, \ldots, a_{\boldsymbol{m}} \rangle = \langle h_1(i), \ldots, h_{\boldsymbol{m}}(i) \rangle$$

Indichiamo con $\mathfrak{R}$ la collezione di tutte le $\mathcal{R}$ elencabili.

Mentre è chiaro che $\mathfrak{D} \subseteq \mathfrak{E} \subseteq \mathfrak{R}$, è stato arduo stabilire che *non* si trattava di inclusioni *strette*.

Definizioni esistenziali di coefficiente binomiale

ecc.

Esempi di scala media

$$\binom{r}{j} = \left\lfloor \frac{(u+1)^r}{u^j} \right\rfloor \% \, u \quad \text{per ogni } u \geqslant 2^r + 0^{r+j}$$

$$j\,! = \left\lfloor \frac{r^j}{\binom{r}{j}} \right\rfloor \quad \text{per ogni } r > (2\,j)^{j+1}$$

$$\neg \exists\, x \exists\, y \left(p = (x+2)\,(y+2) \vee p = 0 \vee p = 1 \right)$$
$$\iff \exists\, q \exists\, u \exists\, v \left(p = 2 + q \;\&\; p\,u - (q+1)!\,v = 1 \right)$$

Fig. 1. Coefficiente binomiale, fattoriale, e "p è un primo" sono diofantei esponenziali, cfr. [Rob52, pp. 446–447]. Dappertutto, '%' designa l'operazione *resto* sugli interi.

Esempi di scala media

$$\binom{r}{j} = \left\lfloor \frac{(u+1)^r}{u^j} \right\rfloor \% \, u \quad \text{per ogni } u \geqslant 2^r + 0^{r+j}$$

$$j\,! = \left\lfloor \frac{r^j}{\binom{r}{j}} \right\rfloor \quad \text{per ogni } r > (2\,j)^{j+1}$$

$$\begin{aligned}
&\neg\,\exists\, x\,\exists\, y\,\big(p = (x+2)\,(y+2) \vee p = 0 \vee p = 1\big)\\
\iff\ &\exists\, q\,\exists\, u\,\exists\, v\,\big(p = 2+q\ \&\ p\,u - (q+1)!\,v = 1\big)\\
\iff\ &\exists\, q\,\exists\, u\quad \big(p = 2+q\ \&\ p\,u = (q+1)!\quad +1\big)\\
\iff\ &\exists\, q\,\exists\, u\quad \left(p = 2+q\cdot 0^{\left((q+1)!+1-(2+q)\,u\right)^2}\right)
\end{aligned}$$

Fig. 1. Coefficiente binomiale, fattoriale, e "p è un primo" sono diofantei esponenziali, cfr. [Rob52, pp. 446–447]. Dappertutto, '%' designa l'operazione *resto* sugli interi.

Esempi di scala media

$$\binom{r}{j} = \left\lfloor \frac{(u+1)^r}{u^j} \right\rfloor \% \, u \quad \text{per ogni } u \geqslant 2^r + 0^{r+j}$$

$$j\,! = \left\lfloor \frac{r^j}{\binom{r}{j}} \right\rfloor \quad \text{per ogni } r > (2\,j)^{j+1}$$

$$\begin{aligned}
&\neg \exists x \, \exists y \, \big(p = (x+2)\,(y+2) \vee p = 0 \vee p = 1 \big) \\
\iff &\exists q \, \exists\, u \, \exists v \, \big(p = 2 + q \;\&\; p\,u - (q+1)!\,v = 1 \big) \\
\iff &\exists q \, \exists\, u \quad \big(p = 2 + q \;\&\; p\,u = (q+1)! \quad + 1 \big) \\
\iff &\exists q \, \exists\, u \quad \left(p = 2 + q \cdot 0^{\left((q+1)! + 1 - (2+q)\,u \right)^2} \right)
\end{aligned}$$

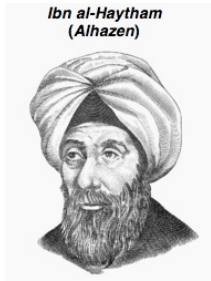


Fig. 1. Coefficiente binomiale, fattoriale, e "p è un primo" sono diofantei esponenziali, cfr. [Rob52, pp. 446–447]. Dappertutto, '%' designa l'operazione *resto* sugli interi.

Esercizio

Spiegare queste specifiche della primalità sfruttando lemma di Bézout e teorema di Wilson.

Relazioni a crescita esponenziale

“ $\mathfrak{c}$ è una potenza del 2 ” [Rob69]

$$
\begin{aligned}
& \exists\, \ell \;\; 2^{\ell} = \mathfrak{c} \\
\iff \quad & \forall\, u \leqslant \mathfrak{c} \;\; \forall\, v \leqslant \mathfrak{c} \quad \mathfrak{c} \neq (2\,u+3)\cdot v \\
\iff \quad & \forall\, u \leqslant \mathfrak{c} \;\; \forall\, v \leqslant \mathfrak{c} \quad \exists\, w \left[\mathfrak{c} - (2\,u+3)\cdot v\right]^2 = 1 + w
\end{aligned}
$$

" $\mathfrak{c}$ È UNA POTENZA DEL 2 " [ROB69]

$$
\begin{aligned}
& \exists\, \ell \;\; 2^{\ell} = \mathfrak{c} \\
\iff \quad & \forall\, u \leqslant \mathfrak{c} \;\; \forall\, v \leqslant \mathfrak{c} \quad \mathfrak{c} \neq (2u+3)\cdot v \\
\iff \quad & \forall\, u \leqslant \mathfrak{c} \;\; \forall\, v \leqslant \mathfrak{c} \quad \exists\, w \left[\mathfrak{c} - (2u+3)\cdot v\right]^2 = 1 + w \\
\iff \quad & \exists\, \ell \exists\, s \exists\, d \Big[\;\; 1 = s \,\%\, \big(1 + d\big) \;\; \& \\
& \qquad\qquad \mathfrak{c} = s \,\%\, \big(1 + (\ell+1)\cdot d\big) \;\; \& \\
& \qquad\qquad \forall i \leqslant \ell \Big[\, s \,\%\, \big(1 + (i+2)\cdot d\big) \;\; = \\
& \qquad\qquad\qquad\qquad 2 \cdot \big[s \,\%\, \big(1 + (i+1)\cdot d\big] \, \Big] \Big] .
\end{aligned}
$$

- L'insieme delle potenze di 2 è diofanteo ?

(Alfred Tarski, 1901–1983)

- L'insieme delle potenze di 2 è diofanteo ?
- Il grafo della funzione $n \mapsto 2^n$ è diofanteo ?

- L'insieme delle potenze di 2 è diofanteo ?
- Il grafo della funzione $\mathfrak{n} \mapsto 2^{\mathfrak{n}}$ è diofanteo ?
- Il grafo della funzione $\langle \mathfrak{b}\,,\ \mathfrak{n} \rangle \mapsto \mathfrak{b}^{\mathfrak{n}}$ è diofanteo ?

- L'insieme delle potenze di 2 è diofanteo ?
- Il grafo della funzione $\mathfrak{n} \mapsto 2^{\mathfrak{n}}$ è diofanteo ?
- Il grafo della funzione $\langle \mathfrak{b}\,,\, \mathfrak{n} \rangle \mapsto \mathfrak{b}^{\mathfrak{n}}$ è diofanteo ?

J.R. Che la famiglia $\mathfrak{D}$ delle rel. diofantee $\begin{matrix}\text{includa} \\ \therefore \\ \text{coincida con}\end{matrix}$ quella, $\mathfrak{E}$, di tutte le relazioni diofantee esponenziali ?

Su quale 'indizio' poggia la congettura J.R. ?

L'eq.

$$X^2 - \overbrace{(a^2-1)}^{\mathfrak{d}}\, Y^2 \;=\; 1\,, \qquad \text{con} \quad a \in \mathbb{N}\,,\, a > 1\,,$$

ha in $\mathbb{N}$ le infinite soluzioni $X = x_n(a)$, $Y = y_n(a)$ tali che

$$x_n(a) + y_n(a)\sqrt{\mathfrak{d}} \;=\; \left(a + \sqrt{\mathfrak{d}}\right)^n .$$

Un formidabile intreccio combinatorio lega tra loro queste soluzioni.

Su quale 'indizio' poggia la congettura J.R. ?

L'eq.

$$X^2 - \overbrace{(a^2-1)}^{\mathfrak{d}}\, Y^2 \;=\; 1\,, \qquad \text{con} \quad a \in \mathbb{N}\,,\, a > 1\,,$$

ha in $\mathbb{N}$ le infinite soluzioni $X = x_n(a)$, $Y = y_n(a)$ tali che

$$x_n(a) + y_n(a)\sqrt{\mathfrak{d}} \;=\; \left(a + \sqrt{\mathfrak{d}}\right)^n .$$

Un formidabile intreccio combinatorio lega tra loro queste soluzioni.

Esempio (ca. 1970): Se $y_n^2(a) \mid y_\ell(a)$, allora $y_n(a) \mid \ell$

Supponiamo ora che $\mathcal{J}$ sia una relazione diadica tale che:

1. $\mathcal{J}(u,v) \implies v < u^u$;
2. $\forall k \exists u \exists v \left[\mathcal{J}(u,v) \,\&\, u^k < v \right]$;

Supponiamo ora che $\mathcal{J}$ sia una relazione diadica tale che:

1. $\mathcal{J}(u,v) \implies v < u^u$;
2. $\forall k \exists u \exists v \big[\mathcal{J}(u,v) \,\&\, u^k < v \big]$;
3. $\mathcal{J}(u,v) \implies u > 1$.

Con [Rob52] si inizia a dire che una tale $\mathcal{J}$
ha crescita esponenziale.

Supponiamo ora che $\mathcal{J}$ sia una relazione diadica tale che:

1. $\mathcal{J}(u,v) \implies v < u^u$;
2. $\forall k \exists u \exists v \big[\mathcal{J}(u,v) \,\&\, u^k < v \big]$;
3. $\mathcal{J}(u,v) \implies u > 1$.

Con [Rob52] si inizia a dire che una tale $\mathcal{J}$ ***ha crescita esponenziale***.

Esempio storico

Prendere

$$\mathcal{J} = \Big\{ \langle u, \phi_{2u} \rangle \mid u > 1 \Big\} ,$$

ove

$$\phi_0 = 0, \quad \phi_1 = 1, \quad \phi_{h+2} = \phi_{h+1} + \phi_h ,$$

per $h = 0, 1, 2, \ldots$

Supponiamo ora che $\mathcal{J}$ sia una relazione diadica tale che:

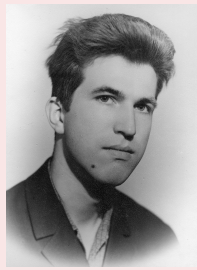
1. $\mathcal{J}(u,v) \implies v < u^u$;
2. $\forall k \exists u \exists v \big[\mathcal{J}(u,v) \,\&\, u^k < v \big]$;
3. $\mathcal{J}(u,v) \implies u > 1$.

Con [Rob52] si inizia a dire che una tale $\mathcal{J}$
ha crescita esponenziale.

Esempio storico ☺ Diofantea! ☺

Prendere

$$\mathcal{J} = \Big\{ \langle u, \phi_{2u} \rangle \mid u > 1 \Big\} ,$$



ove

$$\phi_0 = 0, \quad \phi_1 = 1, \quad \phi_{h+2} = \phi_{h+1} + \phi_h ,$$

per $h = 0, 1, 2, \ldots$ (Vedi [Mat70a])

$$\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c} \Longleftrightarrow (\exists\, a\,,\ d\,,\ \ell\,,\ s\,, x\,,\ h)\Bigg[\ (\mathfrak{c}-1)^2+\mathfrak{n}=0 \quad \vee$$

$$(\mathfrak{n}\geqslant 1\ \&\ \mathfrak{c}+\mathfrak{b}=0) \quad \vee$$

$$\Big(\mathfrak{n}\geqslant 1\ \ \&\ \ \mathfrak{b}\geqslant 1\ \ \&\ \ \boxed{\mathcal{J}(a,d)}\ \ \&\ \ d>\ell \quad \&$$

$$\ell^2=\left(a^2-1\right)\left[(a-1)\,s+\mathfrak{n}\right]^2+1 \quad \&$$

$$x^2=(\mathfrak{b}+\mathfrak{n})^3\,(\mathfrak{b}+\mathfrak{n}+2)\,(h+1)^2+1 \quad \&$$

$$2\,a\,\mathfrak{b}-\mathfrak{b}^2-1\geqslant(\mathfrak{b}+\mathfrak{n}+1)\,x \quad \&\quad a>\mathfrak{b}+\mathfrak{n} \quad \&$$

$$(2\,a\,\mathfrak{b}-\mathfrak{b}^2-1)\,\%\left[\ell-\left(a-\mathfrak{b}\right)\left((a-1)\,s+\mathfrak{n}\right)\right]=\mathfrak{c}\ \Big)\ \Bigg].$$

Il teorema di Davis, Putnam, Robinson

TEOREMA (FORMA NORMALE DI DAVIS 1950 TANTALIZZANTE !)

Data una $\boldsymbol{m}$-upla $\langle h_1, \ldots, h_{\boldsymbol{m}} \rangle$ di funzioni monadiche ricorsive primitive, si può costruire un pol. D a coefficienti interi tale che

$$\langle a_1, \ldots, a_{\boldsymbol{m}} \rangle \in \{ \langle h_1(i), \ldots, h_{\boldsymbol{m}}(i) \rangle : i \in \mathbb{N} \}$$

$$\Longleftrightarrow$$

$$\exists\, y\, \forall\, u \leqslant y\, \exists\, v_1 \leqslant y \cdots \exists\, v_k \leqslant y\; D(a_1, \ldots, a_{\boldsymbol{m}}, y, u, v_1, \ldots, v_k) = 0\,.$$

Teorema (forma normale di Davis 1950 tantalizzante !)

Data una $\boldsymbol{m}$-upla $\langle h_1, \ldots, h_{\boldsymbol{m}} \rangle$ di funzioni monadiche ricorsive primitive, si può costruire un pol. D a coefficienti interi tale che

$$\langle a_1, \ldots, a_{\boldsymbol{m}} \rangle \in \{ \langle h_1(i), \ldots, h_{\boldsymbol{m}}(i) \rangle : i \in \mathbb{N} \}$$

$$\Longleftrightarrow$$

$$\exists y \, \forall u \leqslant y \, \exists v_1 \leqslant y \cdots \exists v_k \leqslant y \; D(a_1, \ldots, a_{\boldsymbol{m}}, y, u, v_1, \ldots, v_k) = 0 .$$

Congettura M.D.: Che la famiglia $\mathfrak{D}$ delle rel. diofantee
includa $\therefore$
coincida con
quella, $\mathfrak{R}$, di tutte le rel. elencabili ?

Elencabilità e '*decidibilità*'

Preistoria del teorema DPR: la P.A.P.

"It was in the summer of 1959 that Hilary and I really hit the jackpot. We decided to see how far we could get $[\cdots]$ if, following Julia Robinson's lead, we were willing to permit variable exponents in our Diophantine equations." *(M.D., 2016)*

$$\boxed{\mathfrak{E} = \mathfrak{R}}$$

2

Preistoria del teorema DPR: la P.A.P.

"It was in the summer of 1959 that Hilary and I really hit the jackpot. We decided to see how far we could get $[\cdots]$ if, following Julia Robinson's lead, we were willing to permit variable exponents in our Diophantine equations." *(M.D., 2016)*

$$\mathfrak{E} = \mathfrak{R}$$

P.A.P.: Esistono progressioni aritmetiche di lunghezza arbitraria interamente costituite da numeri primi.[2] *(M. D. & H.P., 1959)*

[2] Una seq. formata da primi in progressione è, ad es.: $5, 11, 17, 23, 29$.

Preistoria del teorema DPR: la P.A.P.

"It was in the summer of 1959 that Hilary and I really hit the jackpot. We decided to see how far we could get [$\cdots$] if, following Julia Robinson's lead, we were willing to permit variable exponents in our Diophantine equations." *(M.D., 2016)*

$$\mathfrak{E} = \mathfrak{R}$$

P.A.P.: Esistono progressioni aritmetiche di lunghezza arbitraria interamente costituite da numeri primi.[2] *(M. D. & H.P., 1959)*

"It wasn't until 2004 that Ben Green and Terence Tao proved that P.A.P. is true, thus validating our work as a complete proof, but only well after the fact."

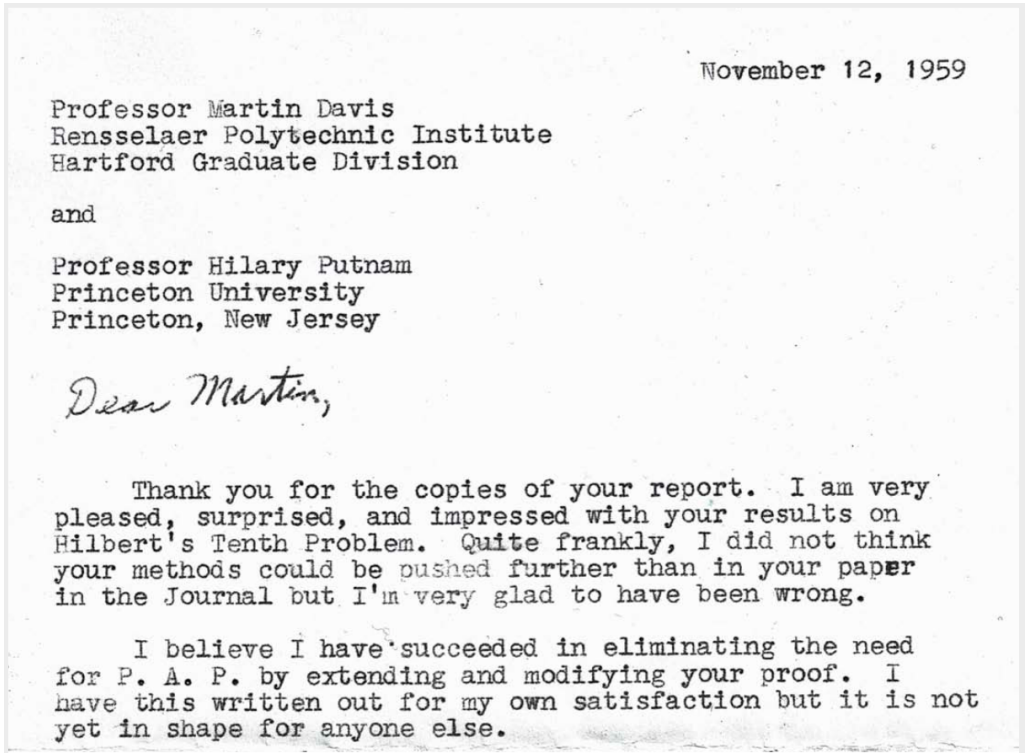
(M.D., 2010)

[2] Una seq. formata da primi in progressione è, ad es.: $5, 11, 17, 23, 29$.

Il teorema DP riscattato dalla P.A.P.

$$\mathfrak{E} = \mathfrak{R}$$

We submitted our work on Hilbert's tenth problem for publication and at the same time sent a copy to Julia Robinson. Julia responded soon afterwards with an exciting letter:



November 12, 1959

Professor Martin Davis
Rensselaer Polytechnic Institute
Hartford Graduate Division

and

Professor Hilary Putnam
Princeton University
Princeton, New Jersey

Dear Martin,

Thank you for the copies of your report. I am very pleased, surprised, and impressed with your results on Hilbert's Tenth Problem. Quite frankly, I did not think your methods could be pushed further than in your paper in the Journal but I'm very glad to have been wrong.

I believe I have succeeded in eliminating the need for P. A. P. by extending and modifying your proof. I have this written out for my own satisfaction but it is not yet in shape for anyone else.

(M.D., 2016)

Il teorema DP riscattato dalla P.A.P.

$$\mathfrak{E} = \mathfrak{R}$$

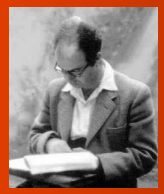
We submitted our work on Hilbert's tenth problem for publication and at the same time sent a copy to Julia Robinson. Julia responded soon afterwards with an exciting letter:

> I am very pleased, surprised, and impressed with your results on Hilbert's tenth problem. Quite frankly, I did not think your methods could be pushed further …
>
> I believe I have succeeded in eliminating the need for [the assumption about primes in arithmetic progression] by extending and modifying your proof.

She sent us her proof soon afterwards; it was a remarkable tour de force. She showed how to get all the primes we needed by using, instead of a then unproved hypothesis about primes in arithmetic progression, the prime number theorem for arithmetic progressions which provided a measure of how frequently primes occurred "on average" in such progressions. We proposed that we withdraw our paper in favor of a joint publication, and she graciously accepted. She undertook the task of writing up the work, and (another surprise), she succeeded in drastically simplifying the proof so only the simplest properties of prime numbers were used.

(M.D., 2016)

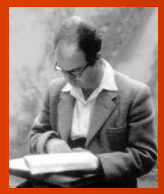
Celebre abbaglio in una recensione di [DPR61]



(Georg Kreisel, 1923–2015)

"*These results are superficially related to Hilbert's tenth Problem on (ordinary, i.e., non-exponential) Diophantine equations. The proof of the authors' results, though very elegant, does not use recondite facts in the theory of numbers nor in the theory of r.e. sets, and so it is likely that the present result is not closely connected with Hilbert's tenth Problem.*

Celebre abbaglio in una recensione di [DPR61]

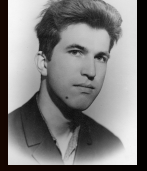


(Georg Kreisel, 1923–2015)

"*These results are superficially related to Hilbert's tenth Problem on (ordinary, i.e., non-exponential) Diophantine equations. The proof of the authors' results, though very elegant, does not use recondite facts in the theory of numbers nor in the theory of r.e. sets, and so it is likely that the present result is not closely connected with Hilbert's tenth Problem. Also it is not altogether plausible that all (ordinary) Diophantine problems are uniformly reducible to those in a fixed number of variables of fixed degree, which would be the case if all r.e. sets were Diophantine.*"

Il teorema di Matiyasevich, sue ricadute

La specifica diofantea del grafo di $\phi_{2\,u}$



Non ancora 23-enne, il matematico russo Yuri Vladimirovich Matiyasevich, dimostrando vera l'ipotesi della Robinson, completa nel 1970 un risultato che ha dei risvolti *piú intriganti* degli stessi teoremi di Gödel del 1931.

$$
\begin{aligned}
u &< v \\
\ell &> v \\
\ell^2 - \ell\, z - z^2 &= 1 \\
g^2 - g\, h - h^2 &= 1 \\
\ell^2 &\mid g \\
\ell &\mid m-2 \\
2\,h+g &\mid m-3 \\
x^2 - m\,x\,y + y^2 &= 1 \\
\ell &\mid x-u \\
2\,h+g &\mid x-v
\end{aligned}
$$

Egli mostra che questo sistema ha soluzione per

$$\begin{matrix} \boldsymbol{u} & \boldsymbol{v} \\ \downarrow & \downarrow \\ u & v \end{matrix}$$

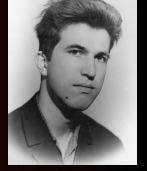
quei valori che sono legati dalla relaz. JR

$$\phi_{2\,\boldsymbol{u}} \;=\; \boldsymbol{v} \quad (\text{con } \boldsymbol{u} > 1)\,,$$

dove $\phi_0 = 0\,, \quad \phi_1 = 1\,,$

$$\phi_{h+2} = \phi_{h+1} + \phi_h\,.$$

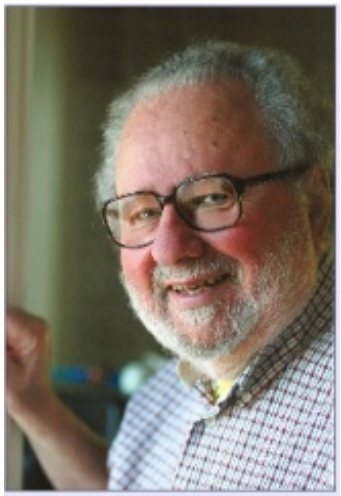
La specifica diofantea del grafo di $\phi_{2\,u}$



Non ancora 23-enne, il matematico russo Yuri Vladimirovich Matiyasevich, dimostrando vera l'ipotesi della Robinson, completa nel 1970 un risultato che ha dei risvolti *piú intriganti* degli stessi teoremi di Gödel del 1931.

$$
\begin{aligned}
(w+1-v+u)^2 &+\\
(a+1+v-\ell)^2 &+\\
(\ell^2-\ell z-z^2-1)^2 &+\\
(g^2-g h-h^2-1)^2 &+\\
(g-b\,\ell^2)^2 &+\\
(m-2-f\,\ell\ )^2 &+\\
(m-3-c\,(2h+g))^2 &+\\
(x^2-m x y+y^2-1)^2 &+\\
(x-u-d\,\ell)^2 &+\\
(x-v-e\,(2h+g))^2 &= 0
\end{aligned}
$$

Fig. In all of these equations, variables range over $\mathbb{N}$. Equations (I)–(X) with parameters u, v, a have a solution for $a > 1$ if and only if $v = y_u(a)$, where $X = x_u(a), Y = y_u(a)$ is the $u+1$st solution, over $\mathbb{N}$, of the Pell equation $X^2 - (a^2-1)Y = 1$. Equations (I)–(XV) with parameters α, β, u have a solution for $\beta \geq 1$ if and only if $\alpha = \beta^u$



Martin Davis

(I)	$u + j = v$
($\mathrm{II_a}$)	$p + (a-1)\,q = v + r + 1$
($\mathrm{II_b}$)	$g = v + t + 1$
(III)	$p^2 - (a^2-1)\,q^2 = 1$
($\mathrm{IV_a}$)	$h + (a+1)\,g = b\,(p + (a+1)\,q)^2$
($\mathrm{IV_b}$)	$h + (a-1)\,g = c\,(p + (a-1)\,q)^2$
(V)	$h^2 - (a^2-1)\,g^2 = 1$
(VI)	$m = (h + (a+1)\,g)\,z + a$
(VII)	$m = (p + (a-1)\,q)\,f + 1$
(VIII)	$x^2 - (m^2-1)\,y^2 = 1$
(IX)	$y = d\,(p + (a-1)\,q) + u$
(X)	$y = e\,(h + (a+1)\,g) + v$
(XI)	$w^2 - (a^2-1)\,v^2 = 1$
(XII)	$(w - (a-\beta)\,v - \alpha)^2 = \gamma^2\,(2a\beta - \beta^2 - 1)^2$
(XIII)	$\alpha + \tau + 1 = 2a\beta - \beta^2 - 1$
(XIV)	$\eta = \beta + \zeta + 1 = u + \xi + 1$
(XV)	$a^2 - (\eta^2-1)\,(\eta-1)^2\,(\delta+1)^2 = 1$

L'esponenziazione definita in poche incognite [MR75]

$$y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$$

$$\begin{aligned}
U &= \mathsf{pell}\Big(\mathfrak{a},\ 2\,(i+1)\,y^2\,\mathsf{pell}\big(\mathfrak{a},\ y\big)\Big)\\
H &= \mathfrak{n} + 2\,y\,j\\
\square &= U\,\mathsf{pell}\big(\mathfrak{a},\ y\big)\,\mathsf{pell}\big(U\,(U-\mathfrak{a})+\mathfrak{a},\ H\big)\\
U &\mid H - y\\
\mathfrak{n} &\leqslant y
\end{aligned}$$

$$\mathrm{pell}(a, u) =_{\mathrm{Def}} (a^2 - 1)\, v^2 + 1$$

$$y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$$

$$\begin{array}{rcl} U & = & \mathrm{pell}\Big(\mathfrak{a},\ 2\,(i+1)\,y^2\,\mathrm{pell}\big(\mathfrak{a},\ y\big)\Big) \\ H & = & \mathfrak{n} + 2\,y\,j \\ \square & = & U\,\mathrm{pell}\big(\mathfrak{a},\ y\big)\,\mathrm{pell}\big(U\,(U-\mathfrak{a})+\mathfrak{a},\ H\big) \\ U & \mid & H - y \\ \mathfrak{n} & \leqslant & y \end{array}$$

$$\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c} \iff \mathfrak{c} = \left\lfloor \frac{\boldsymbol{y}_{\mathfrak{n}+1}(\ 8\,\mathfrak{b}\,(\mathfrak{n}+1)\ \boldsymbol{y}_{\mathfrak{n}+1}(\mathfrak{b}+1)+2\ )}{\boldsymbol{y}_{\mathfrak{n}+1}(\ 8\ \ (\mathfrak{n}+1)\ \boldsymbol{y}_{\mathfrak{n}+1}(\mathfrak{b}+1)\ \ \ )} \right\rfloor$$

Reprimenda dell'abbaglio di Kreisel

Given a polynomial P, we shall construct another polynomial $\overline{P}$ such that

$$P(\, a_1, \ldots, a_\mu \,,\, z_0, \ldots, z_\nu \,) \;=\; 0$$

for some $z_0, \ldots, z_\nu$ if and only if

$$\overline{P}(\, a_1, \ldots, a_\mu \,,\, b, c, d, e, f, g, h, i, j, k, l, m, n \,) \;=\; 0$$

for some $b, c, d, e, f, g, h, i, j, k, l, m, n$.

[MR75, pagg. 521, 522]

Reprimenda dell'abbaglio di Kreisel

Given a polynomial P, we shall construct another polynomial $\overline{P}$ such that

$$P(\, a_1, \ldots, a_\mu \,,\, z_0, \ldots, z_\nu \,) \;=\; 0$$

for some $z_0, \ldots, z_\nu$ if and only if

$$\overline{P}(\, a_1, \ldots, a_\mu \,,\, b, c, d, e, f, g, h, i, j, k, l, m, n \,) \;=\; 0$$

for some $b, c, d, e, f, g, h, i, j, k, l, m, n$.

$$[\cdots]$$

Thus, our theorem shows that every diophantine set is the non-negative part of the range on $\mathbb{N}$ of a polynomial with 14 variables. [MR75, pagg. 521, 522]

All this attention has been gratifying but also embarrassing. What I really am is a mathematician. Rather than being remembered as the first woman
this or that, I would prefer to be remembered, as
a mathematician should, simply for the theorems
I have proved and the problems I have solved. *(J.R.)*

All this attention has been gratifying but also embarrassing. What I really am is a mathematician. Rather than being remembered as the first woman
this or that, I would prefer to be remembered, as
a mathematician should, simply for the theorems
I have proved and the problems I have solved. *(J.R.)*

Sitografia

- https://www.maa.org/programs/maa-awards/writing-awards/the-autobiography-of-julia-robinson
- https://logic.pdmi.ras.ru/~yumat/Julia/index.html
- http://www.nasonline.org/publications/biographical-memoirs/memoir-pdfs/robinson-julia.pdf
  - http://www.zalafilms.com/films/juliarobinson.html
  - https://www.amazon.com/Julia-Robinson-Hilberts-Tenth-Problem/dp/1568814283
  - http://www.claymath.org/library/annual_report/ar2007/07report_robinson.pdf
- https://www.storyofmathematics.com/20th_robinson.html
- http://www.enciclopediadelledonne.it/biografie/julia-bowan-robinson/
- https://www.sciencenews.org/article/how-julia-robinson-helped-define-limits-mathematical-knowledge
- https://blogs.scientificamerican.com/roots-of-unity/the-surprising-link-between-recreational-math-and-undecidability/
- http://www.msri.org/workshops/955

Voci bibliografiche

Martin Davis, Hilary Putnam, and Julia Robinson.
The decision problem for exponential Diophantine equations.
Annals of Mathematics, Second Series, 74(3):425–436, 1961.

Ju. V. Matijasevič. Enumerable sets are Diophantine.
Soviet Mathematics. Doklady, 11(3):354–358, 1970. (Translated from [Mat70b]).

Yu. V. Matiyasevich. Diofantovost' perechislimykh mnozhestv.
Doklady Akademii Nauk SSSR, 191(2):279–282, 1970.
(Russian. Available in English translation as [Mat70a];
translation reprinted in [Sac03, pp. 269–273]).

Yuri Matijasevič and Julia Robinson.
Reduction of an arbitrary diophantine equation to one in 13 unknowns.
Acta Arithmetica, XXVII:521–553, 1975. Reprinted in [Rob96, p. 235ff.].

Julia Robinson. Existential definability in arithmetic.
Transactions of the American Mathematical Society, 72(3):437–449, 1952.
Reprinted in [Rob96, p. 47ff.].

Julia Robinson. Diophantine decision problems.
In W. J. LeVeque, editor, *Studies in Number Theory*, volume 6 of *Studies in Mathematics*, pages 76–116. Mathematical Association of America, 1969.

Julia Robinson. *The collected works of Julia Robinson*, volume 6 of *Collected Works*.
American Mathematical Society, Providence, RI, 1996.
ISBN 0-8218-0575-4. With an introduction by Constance Reid. Edited and with a foreword by Solomon Feferman. xliv+338 pp.

Gerald E. Sacks, editor. *Mathematical Logic in the 20th Century*.
Singapore University Press, Singapore;
World Scientific Publishing Co., Inc., River Edge, NJ, 2003.

1. $(a-4)\cdot(a-5)\cdot(a-9)=0$
2. $(a-b)^2-9=0$
3. $a^2+b^2=2\cdot a\cdot b+(x+1)^2$
4. $a-3\cdot(10-x)=0$
5. $a-x^2\cdot y=0$
6. $a=2\cdot x$; $\qquad a=2\cdot x+1$
7. $a\cdot x=b$;
   $(a\cdot x+y+1-b)^2+(a-y-z-2)^2=0$
8. $\left(a^2+b^2-c^2\right)^2+(a-x-1)^2+$
   $(b-y-1)^2=0$;
   $a\cdot b\cdot\left[(x+1)^2-(a^2+b^2-c^2)^2\right]=0$
9. $a=(x+2)\cdot(y+2)$
10. $a=\left[2\cdot(x+1)+1\right]\cdot y$
11. $2\cdot a=x^2+x$
12. $a=y+z$ & $b=(2\cdot x+1)\cdot y$
13. $a=x+1$ & $b^2-4\cdot a\cdot c-y^2=0$
14. $(c-a-x)^2+(c-b-y)^2+$
    $\left[(c-a)\cdot(c-b)\right]^2=0$

È vero che x^2+x+41 è numero primo per $x=0,1,\ldots,39$ (mentre uguaglia 41^2 per $x=40$). Però questi valori non sono primi consecutivi: ad es., dopo il quarto di essi, che è 53, manca il 59 e dopo il quinto, che è 61, manca il 67 .

Possiamo esprimere il fatto che d *non* è *un quadrato* richiedendo:

$$\exists\, x\, \exists\, y\, \exists\, z \left[x^2 - d \cdot (y+1)^2 = 1 \;\;\&\;\; d = z + 1 \right];$$

in effetti, per ogni $d \in \mathbb{N}$:

- se $d = 0$, manca z;
- quando $d = \square$ e $d \neq 0$, mancano x ed y;
- se d non è un $\square$, ha un predecessore e l'**equazione di Pell** $X^2 - d\, Y^2 = 1$ ha un'infinità di soluzioni intere.

I coefficienti binomiali $\binom{\ell}{0}, \ldots, \binom{\ell}{\ell}$—e anche i successivi $\binom{\ell}{\ell+1+h}$, che valgono tutti 0—sono le cifre della rappresentazione posizionale in base $2^\ell + 1$ del numero $\left((2^\ell + 1) + 1\right)^\ell = \sum_{i=0}^{\ell} \binom{\ell}{i} (2^\ell + 1)^i$:

ℓ	coefficienti binomiali $\binom{\ell}{i}$						base
0	$\cdots$	0	0	0	0	0	1	2
1	$\cdots$	0	0	0	0	1	1	3
2	$\cdots$	0	0	0	1	2	1	5
3	$\cdots$	0	0	1	3	3	1	9
4	$\cdots$	0	1	4	6	4	1	17
$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
		i=...,5,4,3,2,1,0						

Figura: Sulla specifica diofantea esponenziale dei coefficienti binomiali

Quindi varrà $\binom{\ell}{i} = a$ se e solo se vi sono u, v, w, x, y tali che[3]

$$\begin{aligned} u &= 2^\ell + 1\,, \\ (u+1)^\ell &= w\,u\,u^i + a\,u^i + v\,, \\ v + x + 1 &= u^i\,, \\ a + y + 1 &= u\,. \end{aligned}$$

Piú brevemente, se e solo se:

$$a = \left(\left\lfloor (u+1)^\ell / u^i \right\rfloor \,\%\, u\right) \quad \& \quad u = 2^\ell + 1\ .$$

[3] In questa e in simili circostanze, una congiunzione $\&_{i=1}^{h}\, l_i = r_i$ può sempre venir riscritta come 'somma di quadrati', cosí: $\sum_{i=1}^{h}(l_i^2 + r_i^2) = \sum_{i=1}^{h} 2\,l_i\,r_i$.

La collezione $\mathfrak{P}$ delle ***funzioni ricorsive primitive*** è il piú piccolo[4] insieme di funzioni (totali), ad argomenti e risultato in $\mathbb{N}$:

- cui appartengano tutte le *funzioni iniziali*,
- che sia chiuso per *composizione* e *ricorsione*.

[4] I.e., minimo rispetto all'$\subseteq$.

La collezione $\mathfrak{P}$ delle ***funzioni ricorsive primitive*** è il piú piccolo[4] insieme di funzioni (totali), ad argomenti e risultato in $\mathbb{N}$:

- cui appartengano tutte le *funzioni iniziali*,
- che sia chiuso per *composizione* e *ricorsione*.

Le nostre funzioni ***iniziali*** sono: Le funzioni ovunque *nulle*, la funzione *successivo*:

$$\langle x_1, \ldots, x_n \rangle \overset{O_n}{\longmapsto} 0 \qquad (\ n = 0, 1, \ldots\ ),$$

$$x \overset{S}{\longmapsto} x + 1\,,$$

e tutte le

[4] I.e., minimo rispetto all'$\subseteq$.

La collezione $\mathfrak{P}$ delle ***funzioni ricorsive primitive*** è il piú piccolo[4] insieme di funzioni (totali), ad argomenti e risultato in $\mathbb{N}$:

- cui appartengano tutte le *funzioni iniziali*,
- che sia chiuso per *composizione* e *ricorsione*.

Le nostre funzioni ***iniziali*** sono: Le funzioni ovunque *nulle*, la funzione *successivo*:

$$\langle x_1, \ldots, x_n \rangle \overset{O_n}{\longmapsto} 0 \qquad (\ n = 0, 1 \qquad),$$
$$x \overset{S}{\longmapsto} x + 1\,,$$

e tutte le *proiezioni* associate agli interi positivi:

$$\langle x_1, \ldots, x_n \rangle \overset{I_{n,k}}{\longmapsto} x_k \qquad (\ n \geqslant k \geqslant 1\ ).$$

[4] I.e., minimo rispetto all'$\subseteq$.

Composizione di funzioni

Siano:

f una funzione a k argomenti,

$g_1, \ldots, g_k$ funzioni ad M argomenti.

Cosí si definisce la ***composizione*** h di f con $g_1, \ldots, g_k$:

$$\langle x_1, \ldots, x_M \rangle \overset{h}{\longmapsto} f\big(g_1(x_1, \ldots, x_M), \ldots, g_k(x_1, \ldots, x_M)\big) .$$

Siano:

f una funzione a k argomenti,

$g_1, \ldots, g_k$ funzioni ad M argomenti.

Cosí si definisce la ***composizione*** h di f con $g_1, \ldots, g_k$:

$$\langle x_1, \ldots, x_M \rangle \overset{h}{\longmapsto} f\big(g_1(x_1, \ldots, x_M), \ldots, g_k(x_1, \ldots, x_M)\big) .$$

Esempio. Tramite composizione, da O_1 ed S, si ottengono tutte le funzioni costanti:

$$\overbrace{\mathsf{S}(\cdots \mathsf{S}(}^{c} \ \mathsf{O}_1(\, x \,) \ \overbrace{)\cdots)}^{c} .$$

La ***ricorsione***, quando venga applicata ad f e g tali che

f sia una funzione n–adica
(quando $n = 0$, ciò significa che f è una *costante*)

g sia una funzione $n + 2$ adica

produce la funzione $n + 1$ adica

h tale che:

$$\begin{aligned} h(\vec{x}, 0) &= f(\vec{x}) \\ h(\vec{x}, t+1) &= g\big(t, h(\vec{x}, t), \vec{x}\big) \end{aligned}$$

(Qui $\vec{x} =_{\text{Def}} x_1, \ldots, x_n$)

Intreccio combinatorio che lega le soluzioni di $X^2 - (a^2-1)\,Y^2 = 1$ ove $a > 1$

1. $(2\,a)^i \geqslant \boldsymbol{y}_{i+1}(a) > \boldsymbol{y}_{i+1}(a)/a > \boldsymbol{y}_i(a) \geqslant i$ ed $\boldsymbol{y}_{i+1}(a) \geqslant (2\,a-1)^i$;
2. $\boldsymbol{x}_{i+1}(a) > \boldsymbol{x}_{i+1}(a)/a \geqslant \boldsymbol{x}_i(a) \geqslant a^i > i$ ed
   $a^{2\,i+2} \geqslant (2\,a)^{i+1} > \boldsymbol{x}_{i+1}(a), \quad \boldsymbol{x}_{i+2}(a) > a^{i+2}$;
3. $\boldsymbol{x}_i(a) - (a-b)\,\boldsymbol{y}_i(a) \equiv b^i \ \big(\mathbf{mod}\ 2\,a\,b - b^2 - 1\big)$;
4. $\boldsymbol{y}_i(a) \equiv i \ (\mathbf{mod}\ a-1)$;
5. $(b \geqslant 1\ \&\ a > b^n) \Longrightarrow$
   $[\, b^n = c \Longleftrightarrow c\,\boldsymbol{x}_n(a) \leqslant \boldsymbol{x}_n(a\,b) < (c+1)\,\boldsymbol{x}_n(a)\,]$;
6. $(b \geqslant 1\ \&\ a > b^n) \Longrightarrow$
   $\big[\ \boldsymbol{x}_n(a) \leqslant \boldsymbol{x}_m(a\,b) < a\,\boldsymbol{x}_n(a) \quad \Longleftrightarrow \quad m = n\ \big]$;
7. $\boldsymbol{y}_n(a) \mid \boldsymbol{y}_\ell(a)$ se e solo se $n \mid \ell$; se $\boldsymbol{y}_n^2(a) \mid \boldsymbol{y}_\ell(a)$, allora $\boldsymbol{y}_n(a) \mid \ell$.

Un ago nel pagliaio

Si consideri la progr. di Fibonacci $\phi_0 = 0$, $\phi_1 = 1$,

$$\phi_{h+2} = \phi_{h+1} + \phi_h \ .$$

Matiyasevich osservò che

$$\textit{Se} \quad \phi_i^2 \mid \phi_j \ , \quad \textit{allora} \quad \phi_i \mid j \ .$$

Similmente:

$$\textit{Se} \quad \boldsymbol{y}_i^2(\mathfrak{a}) \mid \boldsymbol{y}_j(\mathfrak{a}) \ , \quad \textit{allora} \quad \boldsymbol{y}_i(\mathfrak{a}) \mid j \ .$$

Un ago nel pagliaio

Si consideri la progr. di Fibonacci $\phi_0 = 0$, $\phi_1 = 1$,

$$\phi_{h+2} = \phi_{h+1} + \phi_h \ .$$

Matiyasevich osservò che

$$\textit{Se} \quad \phi_i^2 \mid \phi_j \ , \quad \textit{allora} \quad \phi_i \mid j \ .$$

Similmente:

$$\textit{Se} \quad \boldsymbol{y}_i^2(\mathfrak{a}) \mid \boldsymbol{y}_j(\mathfrak{a}) \ , \quad \textit{allora} \quad \boldsymbol{y}_i(\mathfrak{a}) \mid j \ .$$

CORRECTIONS

The following corrections should be made in the English translations.

R. A. Bairamov, *Criteria of fundamentality for permutation groups and for transformation semigroups*, Vol. 10 (1969), no. 6, 1414–1416.

On page	line	printed	should be
1414	6	assume only one value in E_k	omit at least one value in E_k
	14	For closed sets, condition (1) takes the form	For subsemigroups of Ω_k condition (1) takes the form
	−5	In [4,5,6] it is shown	From [4,5,6] it follows that
1415	−8	groups	subgroups

Ju. V. Matijasevič, *Enumerable sets are diophantine*, Vol. 11 (1970), no. 2, 354–358.

On page 357, line 8 from the bottom "Siberian" should be "Leningrad", page 358, reference [7] should cite the third edition of 1969.

$$\mathfrak{b}^{\mathfrak{n}}=\mathfrak{c} \iff (\exists\, w\,,\ h\,,\ a\,,\ d\,,\ \ell\,,\ u\,,\ v\,,\ s\,,\ q\,,\ z)\Bigg[$$

$$(\mathfrak{c}-1)^2+\mathfrak{b}+\mathfrak{n}=0 \ \vee\ \mathfrak{c}+\mathfrak{b}+(\mathfrak{n}-z-1)^2=0 \ \vee$$

$$\Big(\mathfrak{b}\geqslant 1\ \&\ \mathfrak{c}=z+1\ \&$$

$$w>\mathfrak{b}\ \&\ w>\mathfrak{n}\ \&\ \boxed{Q(w\,,\ h)=q^2}\ \&\ a\geqslant h\ \&\ a>\mathfrak{c}\ \&$$

$$u^2=(a^2\,\mathfrak{b}^2-1)\,v^2+1\ \&\ \mathfrak{c}\,\ell\leqslant u<(\mathfrak{c}+1)\,\ell\ \&\ \ell\leqslant d\ \&$$

$$\ell^2=(a^2-1)\left(\mathfrak{n}+(a-1)\,s\right)^2+1\ \&\ \boxed{\boxed{\mathcal{J}(a,d)}}\Big)\Bigg]$$

(v. [Rob52]).

$$\mathfrak{b}^{\mathfrak{n}}=\mathfrak{c} \iff (\exists\, w\,,\ h\,,\ a\,,\ d\,,\ \ell\,,\ u\,,\ v\,,\ s\,,\ q\,,\ z)\Bigg[$$

$$(\mathfrak{c}-1)^2+\mathfrak{b}+\mathfrak{n}=0 \ \vee\ \mathfrak{c}+\mathfrak{b}+(\mathfrak{n}-z-1)^2=0 \ \vee$$

$$\Big(\mathfrak{b}\geqslant 1\ \&\ \mathfrak{c}=z+1\ \&$$

$$w>\mathfrak{b}\ \&\ w>\mathfrak{n}\ \&\ \boxed{Q(w\,,\ h)=q^2}\ \&\ a\geqslant h\ \&\ a>\mathfrak{c}\ \&$$

$$u^2=(a^2\,\mathfrak{b}^2-1)\,v^2+1\ \&\ \mathfrak{c}\,\ell\leqslant u<(\mathfrak{c}+1)\,\ell\ \&\ \ell\leqslant d\ \&$$

$$\ell^2=(a^2-1)\left(\mathfrak{n}+(a-1)\,s\right)^2+1\ \&\ \boxed{\boxed{\mathcal{J}(a,d)}}\Big)\Bigg]$$

Qui:

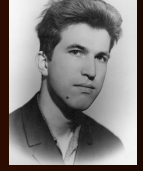
1. $Q(x,y)=\square \implies y>x^x$;
2. $\forall\, x\,\exists\, y\quad Q(x,y)=\square$;

e.g., $Q \leftrightharpoons (x+2)^3\,(x+4)\,(y+1)^2+1$. (V. [MR75])

I would like to say that I expressed my pleasure at finding another Hilbert's tenth problem enthusiast. However, in Julia's sister Constance Reid's memoir, *The Autobiography of Julia Robinson*,[9] based on conversations with Julia shortly before her tragic death of leukemia, she quotes Julia as remembering me saying when we met that I couldn't see how her work "could help solve Hilbert's problem, since it was just a series of examples". I do not want to believe that I said anything so ungracious and so foolish. Julia is also quoted as remembering my "presenting a ten minute paper" at that Congress on my Diophantine results, and as that was not the case, I can comfort myself with the thought that her recollection of what I had said may also have been mistaken.

(M.D., 2016)

Open p.: Does exponentiation admit a single-fold (or at least finite-fold) Diophantine definition ?



"After the DPR-theorem was proved in 1961, in order to establish the existence of Diophantine representations for *every* effectively enumerable set it was sufficient to find a Diophantine representation for *one particular* set of triples

$$\{\langle a, b, c\rangle \quad | \quad a = b^c\} \ . \tag{12}$$

Today we are in a similar position with respect to single-fold (and finite-fold) Diophantine representations: now that we can construct single-fold exponential Diophantine representations for all effectively enumerable sets, in order to transform them into single-fold (or finite-fold) genuinely Diophantine representations, it would be sufficient to find a single-fold (or, respectively, finite-fold) Diophantine representation for the same set of triples (12) ..."

(Yu. Matiyasevich, 2010)