

$$\mathcal{R} \subseteq \mathcal{E}$$

Eugenio G. Omodeo



UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Dip. Matematica e Geoscienze — DMI

Trieste, 20.03.2019
27.03.2019

Sunto

Il teorema di Davis-Putnam-Robinson asserisce che

$$\mathcal{R} \subseteq \mathcal{E}$$

i.e., che ogni insieme *enumerabile ricorsivamente* (in breve 'r.e.')
può essere definito esistenzialmente in termini dell'esponenziazione.

||

Sunto

Il teorema di Davis-Putnam-Robinson asserisce che

$$\mathfrak{R} \subseteq \mathfrak{E}$$

i.e., che ogni insieme *enumerabile ricorsivamente* (in breve 'r.e.') può essere definito esistenzialmente in termini dell'esponenziazione.

|| Ne discende: **Non c'è algoritmo in grado di stabilire, di ogni equaz. diofantea esponenziale, se abbia o no soluzione su \mathbb{N} .**

Rilevanza

La dimostrazione di

$$\mathfrak{R} \subseteq \mathfrak{E}$$

permise di ridurre *all'IPOTESI* J.R. circa l'esistenza di relaz. diofantee polinomiali a crescita esponenziale, \therefore

$$\mathfrak{E} \subseteq \mathfrak{D},$$

contemporaneamente la 'DARING HYPOTHESIS'¹ di [Dav53]

$$\mathfrak{R} \subseteq \mathfrak{D}$$

e il **X di Hilbert**.

¹V. [Mat93, pag. 99]

Scaletta

Dagli insiemi r.e. a quelli esistenzialmente definibili

Un linguaggio di programmazione Turing-completo

Sintassi di un linguaggio Turing-completo

Cenni di semantica e un conveniente azzeramento finale

Emulazione di un programma tramite equaz. esponenziali

Panoramica

Decorso dei valori e tracciato delle attivazioni

Esempio: La congettura di Goldbach ridotta a un'equazione

Insolubilità di H10 riferito a eq. diofantee esponenziali

Inquadramento storico

Dimostrazioni del teorema DPR

Una congettura tardivamente dimostrata

Enunciato del teorema DPR e come affrontarne la dim.

Teorema (Davis-Putnam-Robinson). Sia

$$g : \mathbb{N}^m \longrightarrow \mathbb{N} \cup \{\perp\}$$

una funzione computabile — anche solo parzialmente. Allora il GRAFO di g , i.e.

$$\mathcal{G}(a_0, a_1, \dots, a_m) \leftrightarrow_{\text{Def}} a_0 = g(a_1, \dots, a_m)$$

è una relazione diofantea esponenziale.

Enunciato del teorema DPR e come affrontarne la dim.

Teorema (Davis-Putnam-Robinson). Sia

$$g : \mathbb{N}^m \longrightarrow \mathbb{N} \cup \{\perp\}$$

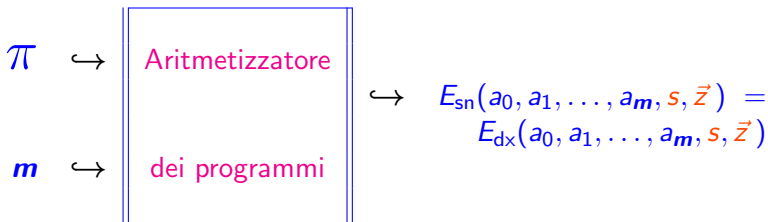
una funzione computabile — anche solo parzialmente. Allora il GRAFO di g , i.e.

$$\mathcal{G}(a_0, a_1, \dots, a_m) \leftrightarrow_{\text{Def}} a_0 = g(a_1, \dots, a_m)$$

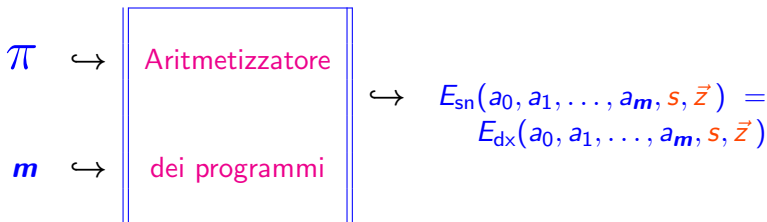
è una relazione diofantea esponenziale.

Dim. (traccia): Per definire esistenzialmente \mathcal{G} , specificheremo tramite equazioni diofantee esponenziali il funzionamento di un programma π computante g . ⊣

Costruz. che dimostrerà, alla Jones-Matiyasevich, il DPR

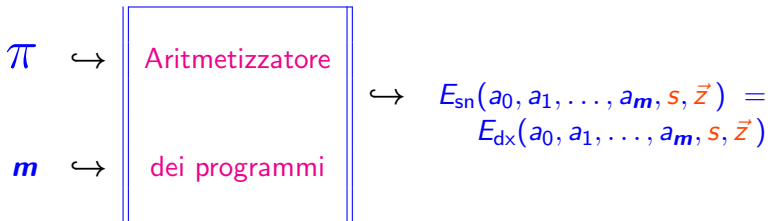


Costruz. che dimostrerà, alla Jones-Matiyasevich, il DPR



L'equazione $E_{\text{sn}} = E_{\text{dx}}$ avrà soluzione, per $\bigwedge_{i=0}^m a_i = \mathbf{a}_i$, sse l'esecuzione di π , avviata sui dati $\mathbf{a}_1, \dots, \mathbf{a}_m$, giunge a **STOP** in un numero $s \in \mathbb{N}$ di passi fornendo a conclusione il risultato \mathbf{a}_0 .

Costruz. che dimostrerà, alla Jones-Matiyasevich, il DPR



L'equazione $E_{\text{sn}} = E_{\text{dx}}$ avrà soluzione, per $\bigwedge_{i=0}^m a_i = \mathbf{a}_i$, sse l'esecuzione di π , avviata sui dati $\mathbf{a}_1, \dots, \mathbf{a}_m$, giunge a **STOP** in un numero $s \in \mathbb{N}$ di passi fornendo a conclusione il risultato \mathbf{a}_0 .

Matiyasevich [Mat74]:

È evitabile che l'eq. $E_{\text{sn}} = E_{\text{dx}}$ sia sotto-determinata.

Dagli insiemi r.e. a quelli esistenzialmente definibili

Un linguaggio di programmazione Turing-completo

Emulazione di un programma tramite equaz. esponenziali
Inquadramento storico

Sintassi di un linguaggio Turing-completo

Cenni di semantica e un conveniente azzeramento finale



Programmazione di una macchina a registri



Introduciamo un LINGUAGGIO DI PROGRAMMAZIONE che
comprende le variabili

R_0, R_1, R_2, \dots (*ad infinitum*)

a valori in \mathbb{N} .

Programmazione di una macchina a registri



Introduciamo un LINGUAGGIO DI PROGRAMMAZIONE che comprende le variabili

R_0, R_1, R_2, \dots (*ad infinitum*)

a valori in \mathbb{N} .

Vi sono istruzioni di cinque sorte, ove $j, k \in \mathbb{N}$:

$R_j \leftarrow R_j + 1$	incremento
$R_j \leftarrow R_j - 1$	decremento
IF $R_j = 0$ GOTO k	salto condizionato
GOTO k	salto <i>in</i> condizionato
STOP	arresto

Programmazione di una macchina a registri

-II

Per PROGRAMMA intendiamo una lista $\mathcal{S}_0, \dots, \mathcal{S}_\ell$ d'istruzioni di dette sorte, con $\ell \in \mathbb{N}$, soggetta alle seguenti limitazioni:



Programmazione di una macchina a registri

-II

Per **PROGRAMMA** intendiamo una lista $\mathfrak{S}_0, \dots, \mathfrak{S}_\ell$ d'istruzioni di dette sorte, con $\ell \in \mathbb{N}$, soggetta alle seguenti limitazioni:

- Quando un'istruzione \mathfrak{S}_i della lista ha la forma
IF $R_j = 0$ **GOTO** k oppure la forma **GOTO** k ,
deve aversi $0 \leq k \leq \ell$ e $k \neq i + 1$; inoltre \mathfrak{S}_k non dev'essere un'istruzione di decremento.

•

•

Programmazione di una macchina a registri

-II

Per PROGRAMMA intendiamo una lista $\mathfrak{S}_0, \dots, \mathfrak{S}_\ell$ d'istruzioni di dette sorte, con $\ell \in \mathbb{N}$, soggetta alle seguenti limitazioni:

-
- Ogni istruzione $R_j \leftarrow R_j - 1$ di decremento dev'essere immediatamente preceduta da un enunciato
IF $R_j = 0$ **GOTO** k , dove il numero k è tenuto, ovviamente, a soddisfare le restrizioni del punto precedente.
-

Programmazione di una macchina a registri

-II

Per PROGRAMMA intendiamo una lista $\mathfrak{S}_0, \dots, \mathfrak{S}_\ell$ d'istruzioni di dette sorte, con $\ell \in \mathbb{N}$, soggetta alle seguenti limitazioni:

- Quando un'istruzione \mathfrak{S}_j della lista ha la forma

IF $R_j = 0$ **GOTO** k oppure la forma **GOTO** k ,
deve aversi $0 \leq k \leq \ell$ e $k \neq i + 1$; inoltre \mathfrak{S}_k non dev'essere un'istruzione di decremento.

- Ogni istruzione $R_j \leftarrow R_j - 1$ di decremento dev'essere immediatamente preceduta da un enunciato

IF $R_j = 0$ **GOTO** k , dove il numero k è tenuto, ovviamente, a soddisfare le restrizioni del punto precedente.

- \mathfrak{S}_ℓ è una **STOP**, l'unica che compare nella lista.

Programmazione di una macchina a registri



Un programma del genere può essere utilizzato per COMPUTARE
una funzione

$$g : \mathbb{N}^m \rightarrow \mathbb{N},$$

totale o parziale (di qui la mezza freccia), ad m operandi, come
segue:

-
-
-
-

Programmazione di una macchina a registri



Un programma del genere può essere utilizzato per COMPUTARE una funzione

$$g : \mathbb{N}^m \rightarrow \mathbb{N},$$

totale o parziale (di qui la mezza freccia), ad m operandi, come segue:

- alle variabili R_1, \dots, R_m vengono assegnati inizialmente i rispettivi valori a_1, \dots, a_m degli OPERANDI;

-
-
-

Programmazione di una macchina a registri



Un programma del genere può essere utilizzato per COMPUTARE una funzione

$$g : \mathbb{N}^m \rightarrow \mathbb{N},$$

totale o parziale (di qui la mezza freccia), ad m operandi, come segue:

-
- le altre var.: R_0, R_{m+1}, \dots, R_r vengono inizialm. poste a 0;
-
-

Programmazione di una macchina a registri



Un programma del genere può essere utilizzato per COMPUTARE una funzione

$$g : \mathbb{N}^m \rightarrow \mathbb{N},$$

totale o parziale (di qui la mezza freccia), ad m operandi, come segue:

-
-
- il programma viene avviato dall'istruzione \mathcal{S}_0 ;
-

Programmazione di una macchina a registri



Un programma del genere può essere utilizzato per COMPUTARE una funzione

$$g : \mathbb{N}^m \rightarrow \mathbb{N},$$

totale o parziale (di qui la mezza freccia), ad m operandi, come segue:

- alle variabili R_1, \dots, R_m vengono assegnati inizialmente i rispettivi valori a_1, \dots, a_m degli OPERANDI;
- le altre var.: R_0, R_{m+1}, \dots, R_r vengono inizialm. poste a 0;
- il programma viene avviato dall'istruzione \mathcal{S}_0 ;
- ecc. ecc.;

Programmazione di una macchina a registri

-IV

- se e quando il programma giunge all'istruzione **STOP**, si prende come **RISULTATO** $g(\mathbf{a}_1, \dots, \mathbf{a}_m)$ il valore conservato nella variabile R_0 ;
-

Programmazione di una macchina a registri

-IV

- se e quando il programma giunge all'istruzione **STOP**, si prende come **RISULTATO** $g(\mathbf{a}_1, \dots, \mathbf{a}_m)$ il valore conservato nella variabile R_0 ;
- (g non associa alcun valore alla m -upla $\mathbf{a}_1, \dots, \mathbf{a}_m$ sse, quando avviato su tali valori, il programma prosegue per sempre).

Terminazione 'pulita' di un progr. della macchina a registri

Esercizio. Mostrare che se c'è un programma π che computa una certa funzione g , allora ce n'è uno che computa la stessa g e che, quando (e se) termina, lascia a 0 tutte le variabili distinte dalla R_0 .

Terminazione 'pulita' di un progr. della macchina a registri

Esercizio. Mostrare che se c'è un programma π che computa una certa funzione g , allora ce n'è uno che computa la stessa g e che, quando (e se) termina, lascia a 0 tutte le variabili distinte dalla R_0 .

Nota Bene. Nel seguito considereremo un programma che termina a questo modo.

Confronto fra 'dialetti' di Shepherdson–Sturgis

Esercizio. Mostrare che l'aggiunta di una nuova sorta d'istruzione, la

IF $R_j \neq 0$ **GOTO** k ,

(di ovvio significato) non aumenterebbe il potere espressivo del linguaggio di programmazione e che anche l'istruzione di salto incondizionato è—noto che sia m —eliminabile.

Come tradurre in \mathcal{E} un programma π , quale ad es.

\mathcal{E}

Prodotto di due numeri

```
0  IF R2 = 0  GOTO  11
1  R2 ← R2 - 1
2  IF R1 = 0  GOTO  7
3  R1 ← R1 - 1
4  R3 ← R3 + 1
5  R0 ← R0 + 1
6  GOTO  2
7  IF R3 = 0  GOTO  0
8  R3 ← R3 - 1
9  R1 ← R1 + 1
10 GOTO  7
```

$\ell = 14$

```
11 IF R1 = 0  GOTO  14
12 R1 ← R1 - 1
13 GOTO  11
STOP
```

$\ell = 2,$
 $r = 3$

Incognite del sistema in cui tradurremo π

s : Numero di passi (ove $< \infty$) che precedono STOP

τ_j : Decorso dei valori di ciascuna var. di programma R_j



l_j : Tracciato delle attivazioni di ciascuna istruzione \mathcal{S}_j



Incognite del sistema in cui tradurremo π

s : Numero di passi (ove $< \infty$) che precedono STOP

τ_j : Decorso dei valori di ciascuna var. di programma R_j

- ▶ i.e., la sequenza $\tau_{j,0}, \dots, \tau_{j,s}$ costituita dall'iniziale $\tau_{j,0}$ e dai susseguenti valori $\tau_{j,t}$ della R_j , ove $\tau_{j,t}$ è il valore súbito dopo l'esecuzione del t -esimo passo.

l_j : Tracciato delle attivazioni di ciascuna istruzione \mathcal{S}_j

▶

Incognite del sistema in cui tradurremo π

s : Numero di passi (ove $< \infty$) che precedono STOP

- τ_j : Decorso dei valori di ciascuna var. di programma R_j
- ▶ i.e., la sequenza $\tau_{j,0}, \dots, \tau_{j,s}$ costituita dall'iniziale $\tau_{j,0}$ e dai susseguenti valori $\tau_{j,t}$ della R_j , ove $\tau_{j,t}$ è il valore súbito dopo l'esecuzione del t -esimo passo.
- l_i : Tracciato delle attivazioni di ciascuna istruzione \mathfrak{S}_i
- ▶ i.e., la sequenza $l_{i,0}, \dots, l_{i,s}$ di 0 / 1 che soddisfa $l_{i,t} = 1$ in corrispondenza di quei t per cui \mathfrak{S}_i è l'istruzione eseguita al $t + 1$ -esimo passo di π .

Incognite del sistema in cui tradurremo π

s : Numero di passi (ove $< \infty$) che precedono STOP

τ_j : Decorso dei valori di ciascuna var. di programma R_j

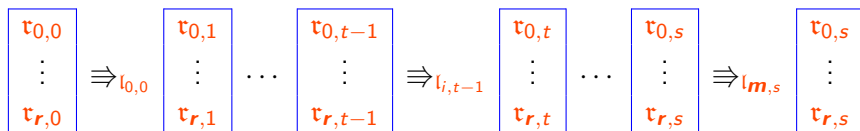
- ▶ i.e., la sequenza $\tau_{j,0}, \dots, \tau_{j,s}$ costituita dall'iniziale $\tau_{j,0}$ e dai susseguenti valori $\tau_{j,t}$ della R_j , ove $\tau_{j,t}$ è il valore subito dopo l'esecuzione del t -esimo passo.

l_i : Tracciato delle attivazioni di ciascuna istruzione \mathfrak{S}_i

- ▶ i.e., la sequenza $l_{i,0}, \dots, l_{i,s}$ di 0 / 1 che soddisfa $l_{i,t} = 1$ in corrispondenza di quei t per cui \mathfrak{S}_i è l'istruzione eseguita al $t + 1$ -esimo passo di π .

Come rappresentare ognuna di queste seq. tramite un numero ?

La **STOP** fa 'quadrare i conti' fra decorsi e tracciati



Solo per una i vale $l_{i,t-1} \neq 0$, a ciascun t

Un'altra incognita del nostro sistema

 sarà la BASE prescelta di un sistema di numerazione posizionale a cifre **molto** 'spaziose'.



Un'altra incognita del nostro sistema

 sarà la BASE prescelta di un sistema di numerazione posizionale a cifre **molto** 'spaziose'.

Questa ci consentirà di assimilare ogni **componente** di ogni v_j a una **cifra** del sistema di numerazione a base **Q**.

Un'altra incognita del nostro sistema

 sarà la BASE prescelta di un sistema di numerazione posizionale a cifre **molto** 'spaziose'.

Questa ci consentirà di assimilare ogni **componente** di ogni r_j a una **cifra** del sistema di numerazione a base Q .

Così potremo utilizzare, semplicemente: come

r_j , quel **numero** che in base Q risulta espresso dalla seq. di **cifre** $r_{j,s} \cdots r_{j,1} r_{j,0}$

Un'altra incognita del nostro sistema

 sarà la BASE prescelta di un sistema di numerazione posizionale a cifre **molto** 'spaziose'.

Questa ci consentirà di assimilare ogni **componente** di ogni r_j a una **cifra** del sistema di numerazione a base Q .

Così potremo utilizzare, semplicemente: come

r_j , quel **numero** che in base Q risulta espresso dalla seq. di **cifre** $r_{j,s} \cdots r_{j,1} r_{j,0}$

l_i , il **numero** analogam. espresso da $l_{i,s} \cdots l_{i,1} l_{i,0}$

Altra incognita ancora (foriera di sotto-determinazione?)

Per comodità, sia Q una potenza positiva del numero 2

Altra incognita ancora (foriera di sotto-determinazione?)

Per comodità, sia Q una potenza positiva del numero 2

Quest'ultimo criterio tira in ballo un altro valore incognito:
quel numero b tale che $Q = 2 \cdot 2^b$

Altra incognita ancora (foriera di sotto-determinazione?)

Per comodità, sia Q una potenza positiva del numero 2

Quest'ultimo criterio tira in ballo un altro valore incognito:
quel numero b tale che $Q = 2 \cdot 2^b$

(È facile rendere b unica tramite un apposito ulteriore vincolo)

$$2^b \neq (2^{a_1} + \dots + 2^{a_m} + 2^s) \max(Q/H/N)$$

$6 + r + \ell$ incognite saranno assoggettate a 4 vincoli più...

s : Numero dei passi che precedono STOP (se è finito)

τ_j : Decorso dei valori di ciascuna var. di programma R_j

l_j : Tracciato delle attivazioni di ciascuna istruzione S_j

Q, b, I : Valori tali che

$$\begin{aligned} 2(a_1 + \dots + a_m + s) < Q = 2 \cdot 2^b > \ell + 1 \\ 1 + (Q - 1)I = Q^{s+1} \end{aligned}$$

dove a_1, \dots, a_m ed a_0 rappresentano i
valori somministrati a π e il corrispettivo risultato

 la BASE prescelta,
 Q a cifre **molto** 'spaziose'.

Evoluz. di stato della memoria : ... $2r + 2$ vincoli piú. . .

$$\begin{pmatrix} \tau_0 \\ \tau_1 \\ \vdots \\ \tau_m \\ \tau_{n+1} \\ \vdots \\ \tau_r \end{pmatrix} = Q \begin{pmatrix} \tau_0 \\ \tau_1 \\ \vdots \\ \tau_m \\ \tau_{n+1} \\ \vdots \\ \tau_r \end{pmatrix} + \Delta \begin{pmatrix} l_0 \\ l_1 \\ \vdots \\ l_\ell \end{pmatrix} + \begin{pmatrix} -Q^{s+1}a_0 \\ a_1 \\ \vdots \\ a_m \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

e $\tau_j \subseteq (\lfloor Q/2 \rfloor - 1) I$ per ogni j , ove

$$\Delta_{j,i} \stackrel{\text{Def}}{=} \begin{cases} 0 & \text{quando } \mathfrak{S}_i \text{ non modifica } R_j, \text{ altrim.} \\ \pm 1 & \text{a seconda che } \mathfrak{S}_i \text{ sia } R_j \leftarrow R_j \pm 1. \end{cases}$$

Flusso di controllo : $\dots 3\ell + 3$ vincoli (al piú)

$$1 \subseteq l_0, \quad l_\ell = Q^s, \quad l_i \subseteq I = \sum_{h=0}^{\ell} l_h \text{ per } i = 0, \dots, \ell - 1;$$

$$Ql_i \subseteq l_{i+1} \quad \text{quando } \mathfrak{S}_i \text{ è di forma } R_j \leftarrow R_j \pm 1;$$

$$Ql_i \subseteq l_k \quad \text{quando } \mathfrak{S}_i \text{ è di forma } \mathbf{GOTO } k;$$

$$Ql_i \subseteq l_{i+1} + l_k \quad \text{quando } \mathfrak{S}_i \text{ è di forma } \mathbf{IF } R_j = 0 \mathbf{ GOTO } k;$$

$$Ql_i \subseteq l_{i+1} + QI - 2r_j \quad \text{quando } \mathfrak{S}_i \text{ è di forma } \mathbf{IF } R_j = 0 \mathbf{ GOTO } k.$$

Flusso di controllo : $\dots 3\ell + 3$ vincoli (al piú)

$$1 \subseteq l_0, \quad l_\ell \subseteq Q^s, \quad l_i \subseteq I = \sum_{h=0}^{\ell} l_h \text{ per } i = 0, \dots, \ell - 1;$$

$$Ql_i \subseteq l_{i+1} \quad \text{quando } \mathfrak{S}_i \text{ è di forma } R_j \leftarrow R_j \pm 1;$$

$$Ql_i \subseteq l_k \quad \text{quando } \mathfrak{S}_i \text{ è di forma } \mathbf{GOTO } k;$$

$$Ql_i \subseteq l_{i+1} + l_k \quad \text{quando } \mathfrak{S}_i \text{ è di forma } \mathbf{IF } R_j = 0 \mathbf{ GOTO } k;$$

$$Ql_i \subseteq l_{i+1} + QI - 2r_j \quad \text{quando } \mathfrak{S}_i \text{ è di forma } \mathbf{IF } R_j = 0 \mathbf{ GOTO } k.$$

Richiamo sulla definibilità esist-/espon-enziale di $a \sqsubseteq b$

Dobbiamo esprimere che $\binom{b}{a}$ è dispari.²

Notiamo che $u > \binom{b}{h}$ quando $u > 2^b$.

Per il *teorema binomiale*:

$$(1 + u)^b = u^{a+1} \sum_{h=a+1}^b \binom{b}{h} u^{h-a-1} + \binom{b}{a} u^a + \sum_{h=0}^{a-1} \binom{b}{h} u^h.$$

Richiediamo che

$$2x + 1 = \left(\left[(u + 1)^b / u^a \right] \% u \right) \wedge u = 2^b + 1.$$

²Grazie al teorema di Lucas.

Senso di $1 + (Q - 1) I = Q^{s+1}$, alla luce di $Q = 2^{b+1} \geq 2$

Mettiamo che potesse essere $Q = 10$. L'unico modo di soddisfare

$$(Q - 1)I = Q^{s+1} - 1$$

sarebbe allora:

$$9 \cdot I = \overbrace{9 \dots 9}^{s+1 \text{ volte}}.$$

Di conseguenza

$$I = \overbrace{1 \dots 1}^{s+1 \text{ volte}} \quad (= \sum_{t=0}^s Q^t);$$

che vale *qualunque sia* $Q > 1$, a patto di leggere gli 1 in base Q .

In base 2 risulterebbe

$$I = \underbrace{0 \dots 0}_b \overbrace{1 \dots 0 \dots 0}_b 1.$$

Vantaggi che derivano dalla $Q = 2^{b+1} \geq 2$

Se esprimiamo posizionalmente due numeri u , v come

$$u = \sum_{i=0}^K u_i Q^i, \quad v = \sum_{i=0}^K v_i Q^i$$

(equiparandone il numero K di cifre Q -arie), allora varrà

$$u \sqsubseteq v \quad \text{se e solo se} \quad u_i \sqsubseteq v_i \quad \text{per} \quad i = 0, 1, \dots, K.$$

Senso delle $\tau_0, \tau_1, \dots, \tau_m, \tau_{m+1}, \dots, \tau_r$

Grazie alla condiz.

$$2(a_1 + \dots + a_m + s) < Q,$$

tenendo conto che il valore $\tau_{j,t}$ assunto da una variabile R_j a qualsiasi istante³ t soddisferà

$$\tau_{j,t} \leq \begin{cases} t + a_j & \text{per } j = 1, \dots, m, \\ t & \text{per } j = 0 \text{ e per } j = m + 1, \dots, r, \end{cases}$$

possiamo rappresentare in base Q il decorso di R_j come

$$\tau_j = \sum_{t=0}^s \tau_{j,t} Q^t,$$

dove $\tau_{j,t} < Q/2 = \lfloor Q/2 \rfloor$.

(($b + 1$)-esimo 'bit' immancabilmente 0)

³Si pensi al tempo scandito dai passi di π .

Istantanee còlte nell'imminenza degli $s + 1$ passi

In base Q , la memoria complessiva si evolve cosí:

$$\begin{pmatrix} \tau_0 \\ \tau_1 \\ \vdots \\ \tau_m \\ \tau_{m+1} \\ \vdots \\ \tau_r \end{pmatrix} = \begin{pmatrix} a_0 & \tau_{0,s-1} & \dots & \tau_{0,1} & 0 \\ 0 & \tau_{1,s-1} & \dots & \tau_{1,1} & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \tau_{m,s-1} & \dots & \tau_{m,1} & a_m \\ 0 & \tau_{m+1,s-1} & \dots & \tau_{m+1,1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \tau_{r,s-1} & \dots & \tau_{r,1} & 0 \end{pmatrix}$$

Questa è una sommaria descrizione qualitativa, di cui abbiamo incontrato qualche lucido fa una precisazione quantitativa.

Senso delle l_0, \dots, l_ℓ

Intendiamo

$$l_{i,t} = \begin{cases} 1 & \text{se l'istruz. al passo } t \text{ è } \mathfrak{S}_i, \\ 0 & \text{se è un'altra,} \end{cases}$$

$$l_i = \sum_{t=0}^s l_{i,t} Q^t,$$

cosicché, in base Q :

$$\begin{pmatrix} l_0 \\ l_1 \\ \vdots \\ l_{\ell-1} \\ l_\ell \end{pmatrix} = \begin{pmatrix} 0 & l_{0,s-1} & \cdots & l_{0,1} & 1 \\ 0 & l_{1,s-1} & \cdots & l_{1,1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & l_{\ell-1,s-1} & \cdots & l_{\ell-1,1} & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

Senso delle l_0, \dots, l_ℓ – Instradamento condizionato

Dalla spiegazione che precede risultano chiari tutti i vincoli sul flusso di controllo, esclusi quelli dell'ultimo tipo — il piú difficile: l'instradamento condizionato.

Instradamento per l'istr. \mathfrak{S}_i : IF $R_j = 0$ GOTO k -

Consideriamo la tabella, formata da 4 righe di $(s + 2) \cdot (b + 1)$ bit:

	$s + 1$	s	t		2	1	0	
$Q l_i$	0	$l_{i,s-1}$...	$l_{i,t-1}$...	$l_{i,1}$	$l_{i,0}$	0
l_{i+1}	0	$l_{i+1,s}$...	$l_{i+1,t}$...	$l_{i+1,2}$	$l_{i+1,1}$	0
$Q I$	1	1	...	1	...	1	1	0
$-2 r_j$	-0	$2 r_{j,s}$...	$2 r_{j,t}$...	$2 r_{j,2}$	$2 r_{j,1}$	$2 r_{j,0}$

La richiesta

$$Q l_i \sqsubseteq l_{i+1} + Q I - 2 r_j \quad (\dagger)$$

è che quando $l_{i,t-1} = 1$, i.e., a $t - 1$ è attiva un'istruz. \mathfrak{S}_i di tipo condizionale, allora a t si attivi \mathfrak{S}_{i+1} oppure l'istruz. rivale, a seconda che valga o meno

$$0 \neq r_{j,t-1} \quad (= r_{j,t}).$$

Instradamento per l'istr. \mathfrak{S}_j : **IF** $R_j = 0$ **GOTO** k **-||**

Preliminarmente si osservi che la sottrazione produce una sequenza

$$QI - 2r_j \quad \left\| \begin{array}{|c|c|c|c|c|c|c|} \hline d_{s+1} & d_s & \cdots & d_t & \cdots & d_2 & d_1 & d_0 \\ \hline \end{array} \right\|$$

di cifre Q -arie dove la parità di d_t è disciplinata, per $t > 0$, dalla regola:

$$d_t \equiv 0 \pmod{2} \quad \text{sse} \quad r_{j,t-1} \neq 0$$

Instradamento per l'istr. \mathfrak{S}_i : **IF** $R_j = 0$ **GOTO** k **-||**

Preliminarmente si osservi che la sottrazione produce una sequenza

$$QI - 2r_j \quad \left\| \begin{array}{|c|c|c|c|c|c|c|} \hline d_{s+1} & d_s & \cdots & d_t & \cdots & d_2 & d_1 & d_0 \\ \hline \end{array} \right\|$$

di cifre Q -arie dove la parità di d_t è disciplinata, per $t > 0$, dalla regola:

$$d_t \equiv 0 \pmod{2} \text{ sse } r_{j,t-1} \neq 0,$$

semplificabile in

$$d_t \equiv 0 \pmod{2} \text{ sse } r_{j,t} \neq 0$$

quando $l_{i,t-1} = 1$, visto che la \mathfrak{S}_i non modifica la memoria.

Instradamento per l'istr. \mathfrak{S}_i : **IF** $R_j = 0$ **GOTO** k -III

Se ad un istante $t - 1 < s$ in cui $l_{i,t-1} = 1$ vale $r_{j,t} = 0$, la parità di $(l_{i+1} + QI - 2r_j)_t$, cioè di $l_{i+1,t} + d_t$, è dunque data da

$$l_{i+1,t} + d_t \not\equiv l_{i+1,t} \pmod{2};$$

così, richiedendo che $l_{i+1,t} + d_t$ sia dispari la (\dagger) impone che $l_{i+1,t} = 0$, cioè che il salto abbia luogo.

Instradamento per l'istr. \mathfrak{S}_i : **IF** $R_j = 0$ **GOTO** k -III

Se ad un istante $t - 1 < s$ in cui $l_{i,t-1} = 1$ vale $r_{j,t} = 0$, la parità di $(l_{i+1} + QI - 2r_j)_t$, cioè di $l_{i+1,t} + d_t$, è dunque data da

$$l_{i+1,t} + d_t \not\equiv l_{i+1,t} \pmod{2};$$

così, richiedendo che $l_{i+1,t} + d_t$ sia dispari la (\dagger) impone che $l_{i+1,t} = 0$, cioè che il salto abbia luogo. Viceversa, se $r_{j,t} \neq 0$, abbiamo

$$l_{i+1,t} + d_t \equiv l_{i+1,t} \pmod{2};$$

così la richiesta che $l_{i+1,t} + d_t$ sia dispari comporta che debba valere $l_{i+1,t} = 1$, che il salto non abbia luogo.

Instradamento per l'istr. \mathfrak{S}_j : IF $R_j = 0$ GOTO k -III

Se ad un istante $t - 1 < s$ in cui $l_{j,t-1} = 1$ vale $r_{j,t} = 0$, la parità di $(l_{i+1} + QI - 2r_j)_t$, cioè di $l_{i+1,t} + d_t$, è dunque data da

$$l_{i+1,t} + d_t \not\equiv l_{i+1,t} \pmod{2};$$

così, richiedendo che $l_{i+1,t} + d_t$ sia dispari la (\dagger) impone che $l_{i+1,t} = 0$, cioè che il salto abbia luogo. Viceversa, se $r_{j,t} \neq 0$, abbiamo

$$l_{i+1,t} + d_t \equiv l_{i+1,t} \pmod{2};$$

così la richiesta che $l_{i+1,t} + d_t$ sia dispari comporta che debba valere $l_{i+1,t} = 1$, che il salto non abbia luogo. In ogni caso, la (\dagger) ben modella l'instradamento esercitato dall'istruzione \mathfrak{S}_j in esame

Vincolo sull'evoluzione di stato della memoria —

Direttamente dalla definizione $\tau_j =_{\text{Def}} \sum_{t=0}^s \tau_{j,t} Q^t$ discende

$$\tau_j - Q \tau_j = \tau_{j,0} + \sum_{t=1}^s (\tau_{j,t} - \tau_{j,t-1}) Q^t - \tau_{j,s} Q^{s+1}$$

Vincolo sull'evoluzione di stato della memoria -|

Direttamente dalla definizione $r_j =_{\text{Def}} \sum_{t=0}^s r_{j,t} Q^t$ discende

$$r_j - Q r_j = r_{j,0} + \sum_{t=1}^s (r_{j,t} - r_{j,t-1}) Q^t - r_{j,s} Q^{s+1},$$

dove

$$r_{j,t} - r_{j,t-1} = \Delta_{j,i} \quad \text{se } i \text{ è l'indice per cui vale } l_{i,t-1} = 1$$

$$\therefore r_{j,t} - r_{j,t-1} = \sum_{i=0}^{\ell} \Delta_{j,i} l_{i,t-1}.$$

Vincolo sull'evoluzione di stato della memoria -|

Direttamente dalla definizione $r_j =_{\text{Def}} \sum_{t=0}^s r_{j,t} Q^t$ discende

$$r_j - Q r_j = r_{j,0} + \sum_{t=1}^s (r_{j,t} - r_{j,t-1}) Q^t - r_{j,s} Q^{s+1},$$

dove

$$r_{j,t} - r_{j,t-1} = \Delta_{j,i} \quad \text{se } i \text{ è l'indice per cui vale } l_{i,t-1} = 1$$

$$\therefore r_{j,t} - r_{j,t-1} = \sum_{i=0}^{\ell} \Delta_{j,i} l_{i,t-1}.$$

Pertanto

$$r_j - Q r_j = r_{j,0} - r_{j,s} Q^{s+1} + \sum_{i=0}^{\ell} \sum_{t=1}^s \Delta_{j,i} l_{i,t-1} Q^t$$

Vincolo sull'evoluzione di stato della memoria -|

Direttamente dalla definizione $r_j =_{\text{Def}} \sum_{t=0}^s r_{j,t} Q^t$ discende

$$r_j - Q r_j = r_{j,0} + \sum_{t=1}^s (r_{j,t} - r_{j,t-1}) Q^t - r_{j,s} Q^{s+1},$$

dove

$$r_{j,t} - r_{j,t-1} = \Delta_{j,i} \quad \text{se } i \text{ è l'indice per cui vale } l_{i,t-1} = 1$$

$$\therefore r_{j,t} - r_{j,t-1} = \sum_{i=0}^{\ell} \Delta_{j,i} l_{i,t-1}.$$

Pertanto

$$r_j - Q r_j = r_{j,0} - r_{j,s} Q^{s+1} + \sum_{i=0}^{\ell} \sum_{t=1}^s \Delta_{j,i} l_{i,t-1} Q^t$$

e, considerato che quando $\Delta_{j,i} \neq 0$ vale $l_{i,s} = 0$, onde

$$\sum_{t=1}^s l_{i,t-1} Q^t = \sum_{t=0}^s l_{i,t} Q^{t+1} = Q l_i,$$

Vincolo sull'evoluzione di stato della memoria -|

Direttamente dalla definizione $\tau_j =_{\text{Def}} \sum_{t=0}^s \tau_{j,t} Q^t$ discende

$$\tau_j - Q \tau_j = \tau_{j,0} + \sum_{t=1}^s (\tau_{j,t} - \tau_{j,t-1}) Q^t - \tau_{j,s} Q^{s+1},$$

dove

$$\tau_{j,t} - \tau_{j,t-1} = \Delta_{j,i} \quad \text{se } i \text{ è l'indice per cui vale } l_{i,t-1} = 1$$

$$\therefore \tau_{j,t} - \tau_{j,t-1} = \sum_{i=0}^{\ell} \Delta_{j,i} l_{i,t-1}.$$

Pertanto

$$\tau_j - Q \tau_j = \tau_{j,0} - \tau_{j,s} Q^{s+1} + \sum_{i=0}^{\ell} \sum_{t=1}^s \Delta_{j,i} l_{i,t-1} Q^t$$

e, considerato che quando $\Delta_{j,i} \neq 0$ vale $l_{i,s} = 0$, onde

$$\sum_{t=1}^s l_{i,t-1} Q^t = \sum_{t=0}^s l_{i,t} Q^{t+1} = Q l_i,$$

possiamo riscrivere

$$\tau_j - Q \tau_j = \tau_{j,0} - \tau_{j,s} Q^{s+1} + Q \sum_{i=0}^{\ell} \Delta_{j,i} l_i.$$

Vincolo sull'evoluzione di stato della memoria



Per tirar le somme, non serve altro che richiamare:

$$\tau_{j,0} = \begin{cases} 0 & \text{se } j = 0 \vee j > m \\ a_j & \text{se } 0 < j \leq m, \end{cases}$$

$$\tau_{j,s} = \begin{cases} 0 & \text{se } j \neq 0 \\ a_0 & \text{se } j = 0. \end{cases}$$

⊥

Congettura di Goldbach

La congettura di Christian Goldbach (ca. 1742) asserisce che:

“ogni numero pari maggiore di 2 può essere scritto come somma di due primi”.



Congettura di Goldbach espressa come eq. $G(0, x, \vec{z}) = 0$

Si scriva un programma γ che computi la funzione

$$g(a_1) = \begin{cases} 1 & \text{se vi sono numeri primi } p, q \\ & \text{tali che } 2a_1 + 4 = p + q, \\ 0 & \text{altrimenti,} \end{cases}$$

Congettura di Goldbach espressa come eq. $G(0, x, \vec{z}) = 0$

Si scriva un programma γ che computi la funzione

$$g(a_1) = \begin{cases} 1 & \text{se vi sono numeri primi } p, q \\ & \text{tali che } 2a_1 + 4 = p + q, \\ 0 & \text{altrimenti,} \end{cases}$$

utilizzando un procedimento che determini i numeri primi (ad es. http://en.wikipedia.org/wiki/Sieve_of_Eratosthenes).

Conggettura di Goldbach espressa come eq. $G(0, x, \vec{z}) = 0$

Si scriva un programma γ che computi la funzione

$$g(a_1) = \begin{cases} 1 & \text{se vi sono numeri primi } p, q \\ & \text{tali che } 2a_1 + 4 = p + q, \\ 0 & \text{altrimenti,} \end{cases}$$

utilizzando un procedimento che determini i numeri primi (ad es. http://en.wikipedia.org/wiki/Sieve_of_Eratosthenes).

Alla stregua della dimostrazione del teorema DPR, si ricavi da γ un sistema di equazioni diofantee esponenziali —e poi una singola eq. $G(a_0, a_1, \vec{z}) = 0$ — descrivente il grafo $\mathcal{G}(a_0, a_1)$ di g .

Un insieme semidecidibile ma non decidibile

Indichiamo per comodità con ψ_π la funzione monadica

$$\psi_\pi : \mathbb{N} \rightarrow \mathbb{N},$$

totale o parziale, computata da un programma π .

Un insieme semidecidibile ma non decidibile

Indichiamo per comodità con ψ_π la funzione monadica

$$\psi_\pi : \mathbb{N} \rightarrow \mathbb{N},$$

totale o parziale, computata da un programma π .

La teoria dell'enumerabilità ricorsiva ci permette di scrivere un programma κ tale che per ogni altro programma π accade che

$$\{x : \langle x, y \rangle \in \psi_\pi\} \neq \mathbb{N} \setminus \{x : \langle x, y \rangle \in \psi_\kappa\};$$

cioè, i domini delle funz. computate non sono mai complementari.

Un insieme semidecidibile ma non decidibile

Indichiamo per comodità con ψ_π la funzione monadica

$$\psi_\pi : \mathbb{N} \rightarrow \mathbb{N},$$

totale o parziale, computata da un programma π .

In altre parole

$$\mathcal{K} =_{\text{Def}} \{x : \langle x, y \rangle \in \psi_\pi\}$$

è semidecidibile ma non decidibile.

Un insieme semidecidibile ma non decidibile

Indichiamo per comodità con ψ_π la funzione monadica

$$\psi_\pi : \mathbb{N} \rightarrow \mathbb{N},$$

totale o parziale, computata da un programma π .

La teoria dell'enumerabilità ricorsiva ci permette di scrivere un programma \mathcal{K} tale che per ogni altro programma π accade che

$$\{x : \langle x, y \rangle \in \psi_\pi\} \neq \mathbb{N} \setminus \{x : \langle x, y \rangle \in \psi_{\mathcal{K}}\};$$

cioè, i domini delle funz. computate non sono mai complementari.

In altre parole

$$\mathcal{K} =_{\text{Def}} \{x : \langle x, y \rangle \in \psi_{\mathcal{K}}\}$$

è semidecidibile ma non decidibile.

Un insieme semidecidibile ma non decidibile (cont.)

Il Teor. DPR ci permette, poi, di costruire un pol. diofanteo esponenziale parametrico K tale che

$$b = \psi_K(a) \leftrightarrow \exists \vec{z} \quad K(a, b, \vec{z}) = 0;$$

Un insieme semidecidibile ma non decidibile (cont.)

Il Teor. DPR ci permette, poi, di costruire un pol. diofanteo esponenziale parametrico K tale che

$$b = \psi_K(a) \leftrightarrow \exists \vec{z} \quad K(a, b, \vec{z}) = 0;$$

così K risulta esistenzialmente definito dall'equazione

$$K(a, x, \vec{z}) = 0,$$

dove il secondo parametro è stato 'declassato' a nuova incognita.

Un problema algoritmicamente insolubile

Discende di qui l'insolubilità algoritmica del X di Hilbert riferito alle equazioni diofantee esponenziali—anziché a quelle polinomiali.

Un problema algoritmicamente insolubile

Discende di qui l'insolubilità algoritmica del X di Hilbert riferito alle equazioni diofantee esponenziali—anziché a quelle polinomiali.

Ove riuscissimo a risolvere quel problema in totale generalità, potremmo infatti, per qualsiasi assegnato valore \mathbf{a} , stabilire se l'equazione $K(\mathbf{a}, x, \vec{z}) = 0$ abbia o no soluzione.

Un problema algoritmicamente insolubile

Discende di qui l'insolubilità algoritmica del X di Hilbert riferito alle equazioni diofantee esponenziali—anziché a quelle polinomiali.

Ove riuscissimo a risolvere quel problema in totale generalità, potremmo infatti, per qualsiasi assegnato valore \mathbf{a} , stabilire se l'equazione $K(\mathbf{a}, x, \vec{z}) = 0$ abbia o no soluzione.

Ma allora potremmo decidere se \mathbf{a} stia in \mathcal{K} oppure no — contraddizione.

Celebre abbaglio in una recensione di [DPR61]

"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."

[Kre62]

L'aspetto paradossale segnalato da Georg Kreisel

Alla luce del teorema di universalità di Turing, discende dal teorema DPR che

Corollario: Per ogni $m \in \mathbb{N}$, esiste un'equazione diofantea esponenziale

$$U(a_1, \dots, a_m, a_{m+1}, x_1, \dots, x_k) = 0$$

tale che gli insiemi diofantei esponenziali di dimensione n sono tutti e soli gli insiemi definiti da una delle equazioni

$$U(a_1, \dots, a_m, \underline{a}, x_1, \dots, x_k) = 0$$

che risultano dal variare di \underline{a} in \mathbb{N} .

—



Storia della dimostrazione del teorema DPR

- Davis e Putnam dedussero nel 1958 (v. [DP58]) l'asserto

$$\mathfrak{A} \subseteq \mathfrak{E}$$

da una *congettura*, denominata P.A.P.: che vi siano progressioni aritmetiche arbitrariamente lunghe formate per intero da numeri primi

-
-

Storia della dimostrazione del teorema DPR

- Davis e Putnam dedussero nel 1958 (v. [DP58]) l'asserto

$$\mathfrak{A} \subseteq \mathfrak{E}$$

da una *congettura*, denominata P.A.P.: che vi siano progressioni aritmetiche arbitrariamente lunghe formate per intero da numeri primi

- Julia Robinson rese la dimostrazione indipendente da tale congettura nel 1960 (ne risultò [DPR61])
-

Storia della dimostrazione del teorema DPR

- Davis e Putnam dedussero nel 1958 (v. [DP58]) l'asserto

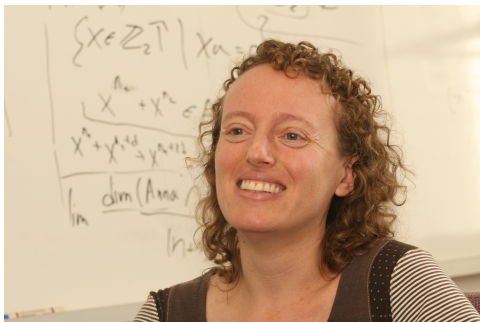
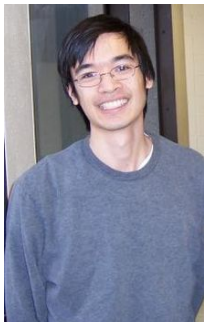
$$\mathfrak{A} \subseteq \mathfrak{E}$$

da una *congettura*, denominata P.A.P.: che vi siano progressioni aritmetiche arbitrariamente lunghe formate per intero da numeri primi

- Julia Robinson rese la dimostrazione indipendente da tale congettura nel 1960 (ne risultò [DPR61])
- Una dimostrazione molto tersa —quella qui presentata sulla scorta di [Dav93]— fu prodotta (tra il 1981 e il 1983) da James Jones e Yuri V. Matiyasevich [JM84]

In merito alla P.A.P.

“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.” [Dav10]



Da una congettura di Davis-Putnam al teor. Tao-Ziegler

In merito alla congettura

“per ogni q , esistono interi positivi r, s tali che i numeri $r, r + s, r + 2s, \dots, r + qs$ risultino tutti primi.”

Da una congettura di Davis-Putnam al teor. Tao-Ziegler

In merito alla congettura

“per ogni q , esistono interi positivi r, s tali che i numeri $r, r + s, r + 2s, \dots, r + qs$ risultino tutti primi.”

Harold N. Shapiro può averne, tramite conversazioni, stimolato l'ideazione (v. [DPR61])

Da una congettura di Davis-Putnam al teor. Tao-Ziegler

In merito alla congettura

“per ogni q , esistono interi positivi r, s tali che i numeri $r, r + s, r + 2s, \dots, r + qs$ risultino tutti primi.”

Harold N. Shapiro può averne, tramite conversazioni, stimolato l'ideazione (v. [DPR61])

Ben Joseph Green & Terence Tao l'hanno dimostrata nel 2004

Da una congettura di Davis-Putnam al teor. Tao-Ziegler

In merito alla congettura

“per ogni q , esistono interi positivi r, s tali che i numeri $r, r + s, r + 2s, \dots, r + qs$ risultino tutti primi.”

Harold N. Shapiro può averne, tramite conversazioni, stimolato l'ideazione (v. [DPR61])

Ben Joseph Green & Terence Tao l'hanno dimostrata nel 2004

Terence Tao & Tamar Debora Ziegler ne hanno dimostrato una formidabile generalizzazione nel 2006 (v. [TZ08]):

Da una congettura di Davis-Putnam al teor. Tao-Ziegler

In merito alla congettura

“per ogni q , esistono interi positivi r, s tali che i numeri $r, r + s, r + 2s, \dots, r + qs$ risultino tutti primi.”

Harold N. Shapiro può averne, tramite conversazioni, stimolato l'ideazione (v. [DPR61])

Ben Joseph Green & Terence Tao l'hanno dimostrata nel 2004

Terence Tao & Tamar Debora Ziegler ne hanno dimostrato una formidabile generalizzazione nel 2006 (v. [TZ08]):

“Dati i polinomi $P_0, P_1, \dots, P_q \in \mathbb{Z}[x]$, con $P_0(0) = P_1(0) = \dots = P_q(0) = 0$, e un $\epsilon > 0$, vi sono infiniti interi r ed s , con $1 \leq s \leq r^\epsilon$, tali che $r + P_0(s), r + P_1(s), \dots, r + P_q(s)$ risultino primi.”

Voci bibliografiche



Martin Davis.

Arithmetical problems and recursively enumerable predicates.
The Journal of Symbolic Logic, 18(1):33–41, 1953.



Martin Davis. *Lecture Notes in Logic*.

Courant Institute of Mathematical Sciences, New York
University, 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 and Hilary Putnam.

Reduction of Hilbert's tenth problem.
The Journal of Symbolic Logic, 23(2):183–187, 1958.



Martin Davis, Hilary Putnam, and Julia Robinson.

The decision problem for exponential Diophantine equations.
Annals of Mathematics, Second Series, 74(3):425–436, 1961.



J. P. Jones and Y. V. Matijasevič.

Register machine proof of the theorem on exponential
Diophantine representation of enumerable sets.
The Journal of Symbolic Logic, 49(3):818–829, 1984.



Georg Kreisel.

A3061: Davis, Martin; Putnam, Hilary; Robinson, Julia. The
decision problem for exponential Diophantine equations.
Mathematical Reviews, 24A(6A):573, 1962.



Yu. V. Matiyasevich.

Sushchestvovanie neèffektiviziruemykh otsenok v teorii èkponentsial'no diofantovykh uravneniĭ.

Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR (LOMI), 40:77–93, 1974.

(Russian. Translated into English as Yu. V. Matiyasevich, Existence of noneffectivizable estimates in the theory of exponential Diophantine equations, *Journal of Soviet Mathematics*, 8(3):299–311, 1977).



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



Terence Tao and Tamar Ziegler.

The primes contain arbitrarily long polynomial progressions. *Acta Mathematica*, 201:213–305, 2008.