

Due esercizi sui linguaggi predicativi

Eugenio G. Omodeo



UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Dip. Matematica e Geoscienze — DMI



Trieste, aprile–maggio 2022



UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- 1 Enunciare in $\overbrace{\text{una teoria del 1}^{\text{o}} \text{ ordine}}$ la
Congettura di Goldbach



- 1 Enunciare in $\overbrace{\text{una teoria del 1}^{\text{o}} \text{ ordine}}$ la
Congettura di Goldbach
 - Discussione



- ① Enunciare in $\overbrace{\text{una teoria del 1}^{\text{o}} \text{ ordine}}$ la
Congettura di Goldbach
- Discussione
 - La soluzione proposta



① Enunciare in $\overbrace{\text{una teoria del 1}^{\text{o}} \text{ ordine}}$ la
Congettura di Goldbach

- Discussione
- La soluzione proposta
- Altre soluzioni proponibili. . .



- ① Enunciare in $\overbrace{\text{una teoria del 1}^{\text{o}} \text{ ordine}}^{\text{un'aritmetica}}$ la
- Congettura di Goldbach
- Discussione
 - La soluzione proposta
 - Altre soluzioni proponibili...
 - ... fra cui una che sfrutti il teorema Davis-Putnam-Robinson



- un'aritmetica
- ① Enunciare in una teoria del 1^o ordine la
Congettura di Goldbach
- Discussione
 - La soluzione proposta
 - Altre soluzioni proponibili. . .
 - . . . fra cui una che sfrutti il teorema Davis-Putnam-Robinson
- ② Modellare un'aritmetica derogando dal suo 'standard'



un'aritmetica

① Enunciare in una teoria del 1^o ordine la

Congettura di Goldbach

- Discussione
- La soluzione proposta
- Altre soluzioni proponibili...
- ... fra cui una che sfrutti il teorema Davis-Putnam-Robinson

② Modellare un'aritmetica derogando dal suo 'standard'

Riferim. bibliografico: [Enderton(2001), pp. 182–197 e 202 segg.]



Interpretando il linguaggio di A_E (v. sotto) nella struttura

$$\mathfrak{N} = (\mathbb{N}, 0; S, +, \cdot, E; <),$$

esprimervi la congettura di **Christian Goldbach** (del 1742):



Interpretando il linguaggio di A_E (v. sotto) nella struttura

$$\mathfrak{N} = (\mathbb{N}, 0; S, +, \cdot, E; <),$$

esprimervi la congettura di **Christian Goldbach** (del 1742):

Ogni numero intero pari $n > 2$ può venir scomposto come

$$n = p + q,$$

con p, q numeri primi.



where A_E is the set consisting of the eleven sentences listed below. (As in the preceding section, $x \leq y$ abbreviates $x < y \vee x = y$.)

Set A_E of Axioms

$$\forall x \quad Sx \neq 0 \quad (S1)$$

$$\forall x \forall y \quad (Sx = Sy \rightarrow x = y) \quad (S2)$$

$$\forall x \forall y \quad (x < Sy \leftrightarrow x \leq y) \quad (L1)$$

$$\forall x \quad x \not< 0 \quad (L2)$$

$$\forall x \forall y \quad (x < y \vee x = y \vee y < x) \quad (L3)$$

$$\forall x \quad x + 0 = x \quad (A1)$$

$$\forall x \forall y \quad x + Sy = S(x + y) \quad (A2)$$

$$\forall x \quad x \cdot 0 = 0 \quad (M1)$$

$$\forall x \forall y \quad x \cdot Sy = x \cdot y + x \quad (M2)$$

$$\forall x \quad xE0 = S0 \quad (E1)$$

$$\forall x \forall y \quad xESy = xEy \cdot x \quad (E2)$$

$$\forall y \quad (y \neq 0 \rightarrow \exists x \quad y = Sx) \quad (S3)$$



where A_E is the set consisting of the eleven sentences listed below. (As in the preceding section, $x \leq y$ abbreviates $x < y \vee x = y$.)

Set A_E of Axioms

$$\forall x \quad Sx \neq 0 \quad (S1)$$

$$\forall x \forall y \quad (Sx = Sy \rightarrow x = y) \quad (S2)$$

$$\forall x \forall y \quad (x < Sy \leftrightarrow x \leq y) \quad (L1)$$

$$\forall x \quad x \not< 0 \quad (L2)$$

$$\forall x \forall y \quad (x < y \vee x = y \vee y < x) \quad (L3)$$

$$\forall x \quad x + 0 = x \quad (A1)$$

$$\forall x \forall y \quad x + Sy = S(x + y) \quad (A2)$$

$$\forall x \quad x \cdot 0 = 0 \quad (M1)$$

$$\forall x \forall y \quad x \cdot Sy = x \cdot y + x \quad (M2)$$

$$\forall x \quad xE0 = S0 \quad (E1)$$

$$\forall x \forall y \quad xESy = xEy \cdot x \quad (E2)$$

$$\forall y \quad (y \neq 0 \rightarrow \exists x \quad y = Sx) \quad (S3)$$



(Raphael Mitchel Robinson ,
1911–1994)



UNIVERSITÀ
DEGLI STUDI DI TRIESTE

where A_E is the set consisting of the eleven sentences listed below. (As in the preceding section, $x \leq y$ abbreviates $x < y \vee x = y$.)

Set A_E of Axioms

$$\forall x \quad Sx \neq 0 \quad (S1)$$

$$\forall x \forall y \quad (Sx = Sy \rightarrow x = y) \quad (S2)$$

$$\forall x \forall y \quad (x < Sy \leftrightarrow x \leq y) \quad (L1)$$

$$\forall x \quad x \not< 0 \quad (L2)$$

$$\forall x \forall y \quad (x < y \vee x = y \vee y < x) \quad (L3)$$

$$\forall x \quad x + 0 = x \quad (A1)$$

$$\forall x \forall y \quad x + Sy = S(x + y) \quad (A2)$$

$$\forall x \quad x \cdot 0 = 0 \quad (M1)$$

$$\forall x \forall y \quad x \cdot Sy = x \cdot y + x \quad (M2)$$

$$\forall x \quad xE0 = S0 \quad (E1)$$

$$\forall x \forall y \quad xESy = xEy \cdot x \quad (E2)$$

$$\forall y \quad (y \neq 0 \rightarrow \exists x \quad y = Sx) \quad (S3)$$

$$\forall^{\mathbb{J}} = \mathbb{N}$$

$$x \xrightarrow{S^{\mathbb{J}}} x + 1$$

⋮

$$(x, y) \xrightarrow{E^{\mathbb{J}}} x^y$$



(Raphael Mitchel Robinson ,
1911–1994)



UNIVERSITÀ
DEGLI STUDI DI TRIESTE

La struttura interpretativa

$$\mathfrak{N} = (\mathbb{N}, 0; S, +, \cdot, E; <),$$

è definita così:



La struttura interpretativa

$$\mathfrak{N} = (\mathbb{N}, 0; S, +, \cdot, E; <),$$

è definita così:

$$\forall^{\mathfrak{N}} = \mathbb{N}, \quad 0^{\mathfrak{N}} = 0,$$



La struttura interpretativa

$$\mathfrak{N} = (\mathbb{N}, 0; S, +, \cdot, E; <),$$

è definita così:

$$\begin{aligned} \forall^{\mathfrak{J}} &= \mathbb{N}, & 0^{\mathfrak{J}} &= 0, & x &\stackrel{S^{\mathfrak{J}}}{\mapsto} x+1, \\ (x, y) &\stackrel{+^{\mathfrak{J}}}{\mapsto} x+y, & (x, y) &\stackrel{\cdot^{\mathfrak{J}}}{\mapsto} xy, & (x, y) &\stackrel{E^{\mathfrak{J}}}{\mapsto} x^y, \end{aligned}$$



La struttura interpretativa

$$\mathfrak{N} = (\mathbb{N}, 0; S, +, \cdot, E; <),$$

è definita così:

$$\forall^{\mathfrak{J}} = \mathbb{N}, \quad 0^{\mathfrak{J}} = 0, \quad x \xrightarrow{S^{\mathfrak{J}}} x + 1,$$

$$(x, y) \xrightarrow{+^{\mathfrak{J}}} x + y, \quad (x, y) \xrightarrow{\cdot^{\mathfrak{J}}} x y, \quad (x, y) \xrightarrow{E^{\mathfrak{J}}} x^y,$$

$$x <^{\mathfrak{J}} y \text{ sse } x < y.$$



Ogni numero intero pari $n > 2$ può venir scomposto come

$$n = p + q,$$

con p, q numeri primi.



$$\forall x \left(\left(x > 0 \ \& \ \exists y \ x = y + y \rightarrow \right. \right. \\ \left. \left. \exists p \exists q \ (x = p + q \ \& \ \text{Pr}(p) \ \& \ \text{Pr}(q)) \right) \right)$$

ove

$$\text{Pr}(X) \stackrel{\text{Def}}{=} ???$$



$$\forall x \left(\text{SS}0 < x \ \& \ \exists y \ x = y + y \rightarrow \right. \\ \left. \exists p \exists q \ (x = p + q \ \& \ \text{Pr}(p) \ \& \ \text{Pr}(q)) \right)$$

ove

$$\text{Pr}(X) \stackrel{\text{Def}}{=} \neg \exists u \exists v \ (X = (u + 2) \cdot (v + 2))$$



$$\forall x \left(S0 < x \ \& \ \exists y \ x = y + y \rightarrow \right. \\ \left. \exists p \exists q \ (x = p + q \ \& \ Pr(p) \ \& \ Pr(q)) \right)$$

ove

$$Pr(X) \stackrel{\text{Def}}{=} \exists u \exists v \ (X = u + v \ \& \ (u \neq S0) \ \& \ (v \neq S0))$$

o anche:

$$Pr(X) \stackrel{\text{Def}}{=} \forall u \forall v \ (X = u \cdot v \rightarrow (u = S0 \leftrightarrow v \neq S0))$$



ALTRE ENUNCIAZ. PROPONIBILI: EQUIVALENTI ?

$$\forall x \forall y \left(\text{SS0} < x \ \& \ x = y + y \rightarrow \right. \\ \left. \exists p \exists q (x = p + q \ \& \ \text{Pr}(p) \ \& \ \text{Pr}(q)) \right)$$

('Pr' come sopra)



ALTRE ENUNCIAZ. PROPONIBILI: EQUIVALENTI ?

$$\forall x \forall y \left(\text{SS0} < x \ \& \ x = y + y \rightarrow \right. \\ \left. \exists p \exists q (x = p + q \ \& \ \text{Pr}(p) \ \& \ \text{Pr}(q)) \right)$$

('Pr' come sopra), oppure

$$\forall x \forall y \left(\text{SS0} < x \ \& \ x = y + y \rightarrow \exists p \exists q \forall u \forall v \left(x = p + q \ \& \right. \right. \\ \left. \left((p = u \cdot v \vee q = u \cdot v) \rightarrow \right. \right. \\ \left. \left. (u = \text{S0} \leftrightarrow v \neq \text{S0}) \right) \right)$$



PROVIAMONE UN'ALTRA ANCORA: EQUIVALENTE ?

$$\forall x \forall y \exists y \left(S S 0 < x \ \& \ x = y + y \rightarrow \right. \\ \left. \exists p \exists q (x = p + q \ \& \ Pr(p) \ \& \ Pr(q)) \right)$$

('Pr' come sopra).



PROVIAMONE UN'ALTRA ANCORA: EQUIVALENTE ?

$$\forall x \forall y \exists y \left(S S 0 < x \ \& \ x = y + y \rightarrow \right. \\ \left. \exists p \exists q (x = p + q \ \& \ Pr(p) \ \& \ Pr(q)) \right)$$

Questo enunciato è banalmente vero in \mathfrak{N} .



PROVIAMONE UN'ALTRA ANCORA: EQUIVALENTE ?

$$\forall x \forall y \exists y \left(S S 0 < x \ \& \ x = y + y \rightarrow \right. \\ \left. \exists p \exists q (x = p + q \ \& \ Pr(p) \ \& \ Pr(q)) \right)$$

Questo enunciato è banalmente vero in \mathfrak{N} . Si prenda come valore per la y , indipendentemente dal val. di x :



PROVIAMONE UN'ALTRA ANCORA: EQUIVALENTE ?

$$\forall x \forall y \exists y \left(S S 0 < x \ \& \ x = y + y \rightarrow \right. \\ \left. \exists p \exists q (x = p + q \ \& \ Pr(p) \ \& \ Pr(q)) \right)$$

Questo enunciato è banalmente vero in \mathfrak{N} . Si prenda come valore per la y , indipendentemente dal val. di x : lo 0.



È QUEST'ALTRA ENUNCIAZIONE È EQUIVALENTE ?

$$\forall z \exists p \exists q \left(z \cdot S S 0 + S S S S 0 = p + q \ \& \ Pm(p) \ \& \ Pm(q) \right)$$

ove



È QUEST'ALTRA ENUNCIAZIONE È EQUIVALENTE ?

$$\forall z \exists p \exists q \left(z \cdot S S 0 + S S S S 0 = p + q \ \& \ Pm(p) \ \& \ Pm(q) \right)$$

ove

$$Pm(X) \stackrel{=_{\text{Def}}}{=} \forall u \forall v (X = u \cdot v \rightarrow X = u \vee X = v) \ \&$$



È QUEST'ALTRA ENUNCIAZIONE È EQUIVALENTE ?

$$\forall z \exists p \exists q \left(z \cdot S S 0 + S S S S 0 = p + q \ \& \ Pm(p) \ \& \ Pm(q) \right)$$

ove

$$Pm(X) \stackrel{=_{\text{Def}}}{=} \forall u \forall v (X = u \cdot v \rightarrow X = u \vee X = v) \ \& \ S 0 < X$$



È QUEST'ALTRA ENUNCIAZIONE È EQUIVALENTE ?

$$\forall z \exists p \exists q \left(z \cdot S S 0 + S S S S 0 = p + q \ \& \ Pm(p) \ \& \ Pm(q) \right)$$

ove

$$Pm(X) \stackrel{=_{\text{Def}}}{=} \forall u \forall v (X = u \cdot v \rightarrow X = u \vee X = v) \ \& \ S 0 < X$$

Qui interviene sapere piú specifico, riguardante

- \aleph

o, quanto meno,



E QUEST'ALTRA ENUNCIAZIONE È EQUIVALENTE ?

$$\forall z \exists p \exists q \left(z \cdot S S 0 + S S S S 0 = p + q \ \& \ Pm(p) \ \& \ Pm(q) \right)$$

ove

$$Pm(X) \stackrel{=_{\text{Def}}}{=} \forall u \forall v (X = u \cdot v \rightarrow X = u \vee X = v) \ \& \ S 0 < X$$

Qui interviene sapere piú specifico, riguardante

- \aleph o, quanto meno,
- una struttura in cui tutti gli assiomi di A_E siano veri



Sfruttando il teorema di

[Davis et al.(1961)Davis, Putnam, and Robinson],

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.

delineare come costruire un'equazione diofantea esponenziale

$G = 0$ che *manca di soluzione* sse la cong. di Goldbach è vera.



- ① Si scriva un programma a registri γ che computi la funzione

$$g(a) \stackrel{\text{Def}}{=} \begin{cases} 1 & \text{se vi sono primi } p, q \\ & \text{tali che } a + a + 4 = p + q, \\ 0 & \text{altrimenti.} \end{cases}$$



- ① Si scriva un programma a registri γ che computi la funzione

$$g(a) \stackrel{=_{\text{Def}}}{=} \begin{cases} 1 & \text{se vi sono primi } p, q \\ & \text{tali che } a + a + 4 = p + q, \\ 0 & \text{altrimenti.} \end{cases}$$

- ② Alla stregua della dimostraz. Jones-Matiyasevich del teorema DPR, si ricavi da γ un sistema di equaz. diofantee esponenziali definente il grafo $\mathcal{G}(b, a)$ di g .



- ① Si scriva un programma a registri γ che computi la funzione

$$g(a) \stackrel{\text{Def}}{=} \begin{cases} 1 & \text{se vi sono primi } p, q \\ & \text{tali che } a + a + 4 = p + q, \\ 0 & \text{altrimenti.} \end{cases}$$

- ② Alla stregua della dimostraz. Jones-Matiyasevich del teorema DPR, si ricavi da γ un sistema di equaz. diofantee esponenziali definente il grafo $\mathcal{G}(b, a)$ di g .
- ③ Si riscriva tale sistema come una singola equazione esponenziale parametrica $G(b, a, y_1, \dots, y_m) = 0$.



- ① Si scriva un programma a registri Υ che computi la funzione

$$g(a) \stackrel{=_{\text{Def}}}{=} \begin{cases} 1 & \text{se vi sono primi } p, q \\ & \text{tali che } a + a + 4 = p + q, \\ 0 & \text{altrimenti.} \end{cases}$$

- ② Alla stregua della dimostraz. Jones-Matiyasevich del teorema DPR, si ricavi da Υ un sistema di equaz. diofantee esponenziali definente il grafo $\mathcal{G}(b, a)$ di g .
- ③ Si riscriva tale sistema come una singola equazione esponenziale parametrica $G(b, a, y_1, \dots, y_m) = 0$.
- ④ La specifica richiesta è

$$\neg \exists x \exists y_1 \dots \exists y_m \quad G(0, x, y_1, \dots, y_m) = 0.$$



- ① Si scriva un programma a registri Υ che computi la funzione

$$g(a) \stackrel{=_{\text{Def}}}{=} \begin{cases} 1 & \text{se vi sono primi } p, q \\ & \text{tali che } a + a + 4 = p + q, \\ 0 & \text{altrimenti.} \end{cases}$$

- ② Alla stregua della dimostraz. Jones-Matiyasevich del teorema DPR, si ricavi da Υ un sistema di equaz. diofantee esponenziali definente il grafo $\mathcal{G}(b, a)$ di g .
- ③ Si riscriva tale sistema come una singola equazione esponenziale parametrica $G(b, a, y_1, \dots, y_m) = 0$.
- ④ La specifica richiesta è

$$\neg \exists x \exists y_1 \dots \exists y_m \quad G(0, x, y_1, \dots, y_m) = 0.$$

(E se sfruttassimo il teorema di Matiyasevich?)





UNIVERSITÀ
DEGLI STUDI DI TRIESTE

ESERCIZIO D'INTERPRETAZIONE

Trovare una struttura interpretativa *significativamente* diversa dall'interpretazione privilegiata (quale?) in cui risultino tutti contemporaneamente veri i segg. enunciati:¹

$$\begin{array}{l} Sx \neq 0 \\ Sx = Sy \rightarrow x = y \\ y \neq 0 \rightarrow \exists x y = Sx \\ \underbrace{SS \cdots S}_{n+1 \text{ volte}} x \neq x \end{array}$$

¹Enunciati davvero? Omessi per brevità quantificatori universali all'inizio.



SOLUZ. DELL'ESERCIZIO D'INTERPRETAZIONE

Possiamo, per $\ell = 1, 2, 3, 4, \dots$, individuare una distinta struttura

$$\mathfrak{Z}_\ell = (\mathbb{Z} \setminus \{-\ell, -2 \cdot \ell, -3 \cdot \ell, \dots\}, \quad , \quad),$$

ove

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

(interi *con segno*).



SOLUZ. DELL'ESERCIZIO D'INTERPRETAZIONE

Possiamo, per $\ell = 1, 2, 3, 4, \dots$, individuare una distinta struttura

$$\mathfrak{Z}_\ell = (\mathbb{Z} \setminus \{-\ell, -2 \cdot \ell, -3 \cdot \ell, \dots\}, 0, \quad),$$

ove

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

(interi *con segno*).



SOLUZ. DELL'ESERCIZIO D'INTERPRETAZIONE

Possiamo, per $\ell = 1, 2, 3, 4, \dots$, individuare una distinta struttura

$$\mathfrak{Z}_\ell = (\mathbb{Z} \setminus \{-\ell, -2 \cdot \ell, -3 \cdot \ell, \dots\}, 0, m \xrightarrow{S^j} m + \ell),$$

ove

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

(interi *con segno*).



SOLUZ. DELL'ESERCIZIO D'INTERPRETAZIONE

Possiamo, per $\ell = 1, 2, 3, 4, \dots$, individuare una distinta struttura

$$\mathfrak{Z}_\ell = (\mathbb{Z} \setminus \{-\ell, -2 \cdot \ell, -3 \cdot \ell, \dots\}, 0, m \xrightarrow{S^j} m + \ell),$$

ove

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

(interi *con segno*).

Il dominio risulta, così, ripartito in una catena isomorfa al dominio \mathbb{N} dei naturali (con l'operazione di incremento unitario) e da $\ell - 1$ catene isomorfe al dominio degli interi (con la stessa operaz.).



SOLUZ. DELL'ESERCIZIO D'INTERPRETAZIONE

Possiamo, per $\ell = 1, 2, 3, 4, \dots$, individuare una distinta struttura

$$\mathfrak{Z}_\ell = (\mathbb{Z} \setminus \{-\ell, -2 \cdot \ell, -3 \cdot \ell, \dots\}, 0, m \xrightarrow{S^j} m + \ell),$$

ove

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

(interi *con segno*).

Il dominio risulta, così, ripartito in una catena isomorfa al dominio \mathbb{N} dei naturali (con l'operazione di incremento unitario) e da $\ell - 1$ catene isomorfe al dominio degli interi (con la stessa operaz.).

Ogni \mathfrak{Z}_ℓ modella gli assiomi della 'teoria del Successore'.



SOLUZ. DELL'ESERCIZIO D'INTERPRETAZIONE

Possiamo, per $\ell = 1, 2, 3, 4, \dots$, individuare una distinta struttura

$$\mathfrak{Z}_\ell = (\mathbb{Z} \setminus \{-\ell, -2 \cdot \ell, -3 \cdot \ell, \dots\}, 0, m \xrightarrow{S^j} m + \ell),$$

ove

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

(interi *con segno*).

Il dominio risulta, così, ripartito in una catena isomorfa al dominio \mathbb{N} dei naturali (con l'operazione di incremento unitario) e da $\ell - 1$ catene isomorfe al dominio degli interi (con la stessa operaz.).

Ogni \mathfrak{Z}_ℓ modella gli assiomi della 'teoria del Successore'.

Si potrebbe andare oltre, e considerare modelli con *infinite* catene isomorfe a \mathbb{Z} , e.g.

$$\mathfrak{R}_\ell = (\mathbb{R} \setminus \{-1, -2, -3, \dots\}, 0, r \xrightarrow{S^j} r + 1),$$

ove \mathbb{R} è l'insieme dei numeri reali.



La teoria del successore vista sopra, come anche la sua variante che incorpora il relatore $<$ di confronto, assiomatizzabile così:

$$\begin{array}{l}
 y \neq 0 \quad \rightarrow \quad \exists x \ y = Sx \\
 x < Sy \quad \leftrightarrow \quad x < y \vee x = y \\
 \quad \quad \quad \neg \quad x < 0 \\
 x < y \quad \vee \quad x = y \quad \vee \quad y < x \\
 x < y \quad \rightarrow \quad \neg \ y < x \\
 x < y \quad \rightarrow \quad y < z \quad \rightarrow \quad x < z
 \end{array}$$

(da chiudersi universalmente !) sono **complete** nel senso che, in esse, ogni enunciato γ è *dimostrabile* o *refutabile*:

$$\{ \text{assiomi} \} \vdash \gamma \quad \text{oppure} \quad \{ \text{assiomi} \} \vdash \neg \gamma .$$

(Vedi [Enderton(2001), pagg. 187–196])



Tenuto conto dell'*enumerabilità effettiva* delle deduzioni da un insieme decidibile di premesse, otteniamo che dette teorie—in quanto complete—sono entrambe *decidibili*.

E. . .



Tenuto conto dell'*enumerabilità effettiva* delle deduzioni da un insieme decidibile di premesse, otteniamo che dette teorie—in quanto complete—sono entrambe *decidibili*.

E...

... che altro si ricava, dalla completezza della teoria, alla luce del teor. di correttezza ?



Si può decidere—vedi [Cegielski and Richard(2001)]—la teoria della struttura

$$\left(\mathbb{N}, \text{paio}_{/2}, \mathbb{A} \right)$$

ove

$$\text{paio} : \mathbb{N}^2 \rightarrow \mathbb{N}$$

è la biiezione di Cantor

$$(x, y) \xrightarrow{\text{paio}} \frac{(x+y) \cdot (x+y+1)}{2} + x$$

e \mathbb{A} è una qualsiasi delle seguenti relazioni o funzioni:

- moltiplicazione,
- divisibilità,
- addizione,
- ordine,
- successore.





Patrick Cegielski and Denis Richard.

Decidability of the theory of the natural integers with the Cantor pairing function and the successor.

Theoretical Computer Science, 257:51–77, 2001.



Martin Davis, Hilary Putnam, and Julia Robinson.

The decision problem for exponential Diophantine equations.

Annals of Mathematics, Second Series, 74(3):425–436, 1961.



Herbert B. Enderton.

A Mathematical Introduction to Logic.

Harcourt/Academic Press, Burlington, MA, USA, 2nd edition, 2001.



James P. Jones, Daihachiro Sato, Hideo Wada, and Douglas Wiens.

Diophantine representation of the set of prime numbers.

Amer. Math. Monthly, 83(6):449–464, 1976.



PUÒ UN POL. COME QUESTO GENERARE I PRIMI ?

$$\begin{aligned} & (K+2) \cdot \left(1 \right. \\ & \quad \left. - (\bullet \cdot Z + H + J - Q)^2 \right. \\ & \quad \left. - \left((G \cdot K + 2 \cdot G + K + 1) \cdot (H + J) + H - Z \right)^2 \right. \\ & \quad \left. - (2 \cdot N + P + Q + Z - E)^2 \right. \\ & \quad \left. - \left(16 \cdot (K+1)^3 \cdot (K+2) \cdot (N+1)^2 + 1 - \bullet^2 \right)^2 \right. \\ & \quad \left. - \left(E^3 \cdot (E+2) \cdot (A+1)^2 + 1 - \bullet^2 \right)^2 \right. \\ & \quad \left. - \left((A^2 - 1) \cdot Y^2 + 1 - X^2 \right)^2 \right. \\ & \quad \left. - \left(16 \cdot \bullet^2 \cdot Y^4 \cdot (A^2 - 1) + 1 - U^2 \right)^2 \right) \end{aligned}$$



PUÒ UN POL. COME QUESTO GENERARE I PRIMI ?

$$- (N + L + \bullet - Y)^2$$

$$- \left(\left((A + U^2 \cdot (U^2 - A))^2 - 1 \right) \cdot (N + 4 \cdot \bullet \cdot Y)^2 + 1 - (X + \bullet \cdot U)^2 \right)^2$$

$$- \left((A^2 - 1) \cdot L^2 + 1 - M^2 \right)^2$$

$$- (A \cdot I + K + 1 - L - I)^2$$

$$- \left(Z + P \cdot L \cdot (A - P) + \bullet \cdot (2 \cdot A \cdot P - P^2 - 1) - P \cdot M \right)^2$$

$$- \left(Q + Y \cdot (A - P - 1) + \bullet \cdot (2 \cdot A \cdot P + 2 \cdot A - P^2 - 2 \cdot P - 2) - X \right)^2$$

$$- \left(P + L \cdot (A - N - 1) + \bullet \cdot (2 \cdot A \cdot N + 2 \cdot A - N^2 - 2 \cdot N - 2) - M \right)^2$$

)



PUÒ UN POL. COME QUESTO GENERARE I PRIMI ?

$$- (N + L + \bullet - Y)^2$$

$$- \left(\left((A + U^2 \cdot (U^2 - A))^2 - 1 \right) \cdot (N + 4 \cdot \bullet \cdot Y)^2 + 1 - (X + \bullet \cdot U)^2 \right)^2$$

$$- \left((A^2 - 1) \cdot L^2 + 1 - M^2 \right)^2$$

$$- (A \cdot I + K + 1 - L - I)^2$$

$$- \left(Z + P \cdot L \cdot (A - P) + \bullet \cdot (2 \cdot A \cdot P - P^2 - 1) - P \cdot M \right)^2$$

$$- \left(Q + Y \cdot (A - P - 1) + \bullet \cdot (2 \cdot A \cdot P + 2 \cdot A - P^2 - 2 \cdot P - 2) - X \right)^2$$

$$- \left(P + L \cdot (A - N - 1) + \bullet \cdot (2 \cdot A \cdot N + 2 \cdot A - N^2 - 2 \cdot N - 2) - M \right)^2$$

)



Idea: Se ne considerino i valori positivi !



UNIVERSITÀ
DEGLI STUDI DI TRIESTE

“Perhaps some industrious reader will construct a shorter prime representing polynomial.”

[Jones et al.(1976) Jones, Sato, Wada, and Wiens, p. 455]

