A.4 (∗) Il teorema cinese

> "In 1931 Gödel [18] revolutionized mathematical logic when he showed that no system of axioms is sufficient to decide all statements of number theory correctly [· · ·]. In the course of the proof, he needed an arithmetically definable way of representing arbitrary finite sequences of natural numbers. Gödel's elementary solution of this problem using the Chinese remainder theorem is a cornerstone of the negative solution of Hilbert's tenth problem." [DMR76][7]

Teorema 17 (Teorema cinese del resto)**.**

Se $q_1, \ldots, q_n, a_1, \ldots, a_n$ *sono interi tali che per* $i = 1, \ldots, n$*:*

- q_j, q_i *sono tra loro coprimi (in simboli,* $q_j \perp q_i$*) per* $j < i$*,*
- $0 \leqslant a_i < q_i$*,*

allora c'è uno ed un sol numero $\boldsymbol{a}$*,* $0 \leqslant \boldsymbol{a} < \prod_{i=1}^{n} q_i$*, tale che*

$$a_i \quad = \quad \boldsymbol{a} \,\%\, q_i \,, \qquad \text{per } i = 1, \ldots, n.$$

[7] Il [18] di quest'epigrafe si riferisce alla voce bibliografica qui indicata come [Göd31].

Dimostrazione. Le n-uple distinte della forma[8]

$$\langle (a \,\%\, q_1), \ldots, (a \,\%\, q_n) \rangle , \quad \text{con } 0 \leqslant a < \textstyle\prod_{i=1}^{n} q_i,$$

sono esattamente $\prod_{i=1}^{n} q_i$—numero pari a quello delle n-uple $a_1, \ldots, a_n$ che soddisfano i vincoli $0 \leqslant a_i < q_i$. Questo perché quando a', a'' con $0 \leqslant a' \leqslant a'' < \prod_{i=1}^{n} q_i$ soddisfano le $(a' \,\%\, q_i) = (a'' \,\%\, q_i)$, cioè $q_i \mid a'' - a'$ per ogni i, la coprimalità fra q_i implica $\prod_{i=1}^{n} q_i \mid a'' - a'$, il che tiene solo se $a' = a''$. ⊣

Lemma 18 (Gödel, 1931)**.**

Se $q, a_1, \ldots, a_n$ sono interi tali che

$$0 \leqslant a_i < q \qquad \textit{per } i = 1, \ldots, n \ ,$$

allora c'è uno ed un sol numero $\boldsymbol{a}$, $0 \leqslant \boldsymbol{a} < \prod_{i=1}^{n}(1 + n!\, q\, i)$, tale che

$$a_i \quad = \quad \boldsymbol{a} \,\%\, (1 + n!\, q\, i), \qquad \textit{per } i = 1, \ldots, n.$$

Dimostrazione. Posto

$$\boldsymbol{b} \quad =_{\text{Def}} \quad n!\, q \ ,$$

per poter ricorrere al Teor. 17, ci basta mostrare la coprimalità $i\boldsymbol{b} + 1 \perp j\boldsymbol{b} + 1$ per $j < i \leqslant n$. In effetti, se p è un numero tale che $p \mid i\boldsymbol{b} + 1$ e $p \mid j\boldsymbol{b} + 1$, allora

$$\mathsf{MCD}\,(p, \boldsymbol{b}) \quad = \quad \mathsf{MCD}\,(p, n!) \quad = \quad 1 \quad \text{e} \quad p \mid (i - j)\, \boldsymbol{b}\,,$$

e quindi $p \mid i - j$, $\ p \leqslant i - j < n$, dal che $p = 1$. ⊣

Corollario 19. *Per ogni $\langle a_1, \ldots, a_n \rangle \in \mathbb{N}^n$, esistono un multiplo $\boldsymbol{b}$ del fattoriale $n!$ e un numero $\boldsymbol{a}$ tali che, per $i = 1, \ldots, n$:*

$$a_i \quad = \quad (\boldsymbol{a} \,\%\, (i\, \boldsymbol{b} + 1)) \ .$$

Dimostrazione. Poiché i multipli $\boldsymbol{b} = n!\, q$ di $n!$ crescono strettamente al crescere di q, lo stesso avviene per ciascuna voce della n-upla

$$\langle 1\boldsymbol{b} + 1, \ldots, n\boldsymbol{b} + 1 \rangle \ ,$$

che dunque prima o poi surclasserà la $\langle a_1, \ldots, a_n \rangle$. Basta rifarsi al Lemma 18. ⊣

Esercizio 139. *Dimostrare che se ℓ, m, a sono interi tali che $0 \leqslant a < \ell$, $1 < m$ e $\ell \perp m$, allora c'è un $\boldsymbol{a} \in \mathbb{N}$ tale che*

$$\begin{aligned} \boldsymbol{a} &\equiv a \pmod{\ell}\,, \\ \boldsymbol{a} &\equiv 1 \pmod{m}\,. \end{aligned}$$

[8] Qui % designa l'operazione 'resto della divisione' fra naturali, con secondo operando $\neq 0$.

A.4.1 Specifica aritmetica di funzioni ricorsive primitive

Le funzioni RICORSIVE PRIMITIVE formano la piú piccola collezione di funzioni (totali) ad argomenti e risultato in $\mathbb{N}$ che comprenda le *funzioni iniziali*

$$\begin{array}{rcll} \langle x_1,\ldots,x_n\rangle & \overset{\mathsf{O}_n}{\longmapsto} & 0 & (\ n=0,1\ )\,, \\ x & \overset{\mathsf{S}}{\longmapsto} & x+1\,, & \\ \langle x_1,\ldots,x_n\rangle & \overset{\mathsf{I}_{n,k}}{\longmapsto} & x_k & (\ n\geqslant k\geqslant 1\ ) \end{array}$$

e sia chiusa rispetto alla *composizione* e alla *ricorsione*, intese come segue.

Composizione: Si dice che h risulta per *composizione* di f con $g_1,\ldots,g_k$, dove:

f è una funzione a k argomenti,
$g_1,\ldots,g_k$ sono funzioni ad M argomenti

se, per ogni M-upla di argomenti:

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

Ricorsione: Si dice che h risulta per *ricorsione* (primitiva) da funzioni f e g aventi n ed $n+2$ argomenti rispettivamente, quando si ha che, per ogni n-upla $\vec{x}=\langle x_1,\ldots,x_n\rangle$:

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

Esercizio 140. *Mostrare che sono ricorsive primitive le operazioni di somma, prodotto, elevamento a potenza, segno, predecessore, distanza.*

Grazie al teorema cinese, vale questa proposizione:

Teorema 20 (Gödel–Davis [Rob69a])**.** *Il grafo $h(a_1,\ldots,a_n)=b$ di una funzione ricorsiva primitiva h può sempre venir espresso tramite una formula aritmetica in cui i quantificatori universali compaiono solo ristretti e nella quale non figura il connettivo $\neg$ di negazione. La quantificazione esistenziale è ammessa senza restrizioni, perché qui assumiamo come simboli primitivi tanto $\exists$ che $\forall$.*

Dimostrazione. Per le funzioni iniziali, la specifica è immediata:

$$\begin{array}{rcl} \mathsf{O}_n(a_1,\ldots,a_n)=b & \rightsquigarrow & b=0\,, \\ \mathsf{S}(a)=b & \rightsquigarrow & b=a+1\,, \\ \mathsf{I}_{n,k}(a_1,\ldots,a_n)=b & \rightsquigarrow & b=a_k\,. \end{array}$$

Quando h risulta per composizione da f con $g_1,\ldots,g_k$, assumendo induttivamente vero l'asserto del teorema per f e per le g_j, intraprendiamo la traduzione cosí:

$$h(a_1,\ldots,a_M)=b \quad \rightsquigarrow \quad \exists\, y_1\cdots\exists\, y_k\big(f(y_1,\ldots,y_k)=b\ \wedge\ \textstyle\bigwedge_{j=1}^{k}\ g_j(a_1,\ldots,a_M)=y_j\big).$$

Quando h risulta per ricorsione da f e g, assumiamo induttivamente vero l'asserto del teorema per f e per g. Osserviamo che, per $\vec{a}$ ed a fissati, la sequenza

$$f(\vec{a}) = u_0,\ u_1 = g(\vec{a}, 0, u_0), \ldots, u_a = g(\vec{a}, a-1, u_{a-1}),\ u_{a+1} = g(\vec{a}, a, u_a)$$

(ove fa comodo tenere una componente finale in eccesso) può venir codificata tramite una qualsiasi coppia u, d tale che

$$u_t \quad = \quad u \,\%\, \big(1 + (t+1)\cdot d\big) \quad \text{per} \quad t = 0, \ldots, a+1$$

(almeno una tal coppia esiste, per il Lemma 18). Traduciamo:

$$\begin{aligned} h(\vec{a}, a) = b \quad \rightsquigarrow \quad \exists\, u\, \exists\, d \Big[\quad & f(\vec{a}) = u \,\%\, \big(1+d\big) \ \wedge\ b = u \,\%\, \big(1 + (a+1)\cdot d\big) \ \wedge \\ & \forall t \leqslant a \Big(u \,\%\, \big(1 + (t+2)\cdot d\big) \ = \\ & \qquad g\Big(\vec{a}\,,\ t\,,\ u \,\%\, \big(1 + (t+1)\cdot d\big)\Big)\ \Big)\Big]. \end{aligned}$$

Di qui è facile eliminare i riferimenti ad f e a g, grazie all'ipotesi induttiva; del pari eliminabile è l'operatore '%' di resto, grazie all'equivalenza aritmetica

$$u \,\%\, (1+v) = r \quad \leftrightarrow \quad \exists\, q\, \exists\, s \big(u = (1+v)\, q + r \ \wedge\ r + s = v\,\big).$$

⊣

Esempio 141. *Una formula che descrive il grafo di* 2^a*—funzione che vale 1 per* $a = 0$ *e vale* $2 \cdot 2^t$ *quando* $a = t+1$*—è questa:*

$$\begin{aligned} 2^a = b \quad \leftrightarrow \quad \exists\, u\, \exists\, d \Big[\quad & 1 = u \,\%\, \big(1+d\big) \ \wedge\ b = u \,\%\, \big(1 + (a+1)\cdot d\big) \ \wedge \\ & \forall t \leqslant a \Big(u \,\%\, \big(1 + (t+2)\cdot d\big) \ = \\ & \qquad 2 \cdot \big[u \,\%\, \big(1 + (t+1)\cdot d\big]\ \Big)\Big]. \end{aligned}$$

Esercizio 142. *Dimostrare che se* P, Q *sono polinomi a coefficienti interi non-negativi, su* $\mathbb{N}$ *si equivalgono le due formule*

$$\begin{aligned} & \boxed{\forall\, t \leqslant a}\, \exists\, u_0 \cdots \exists\, u_k\, \boxed{\forall\, z \leqslant y}\, \exists\, v_1 \cdots \exists\, v_\ell \quad P = Q\,, \\ & \exists\, a_0 \cdots \exists\, a_k\, \exists\, d_0 \cdots \exists\, d_k\, \boxed{\forall\, t \leqslant a\ \forall\, z \leqslant y}\, \exists\, u_0 \cdots \exists\, u_k\, \exists\, v_1 \cdots \exists\, v_\ell \Big[\quad P = Q \ \wedge \\ & \qquad\qquad \textstyle\bigwedge_{j=0}^{k} u_j = a_j \,\%\, \big(1 + (t+1)\, d_j\big)\Big]. \end{aligned}$$

A.5 (∗) Svolgimento degli esercizi

Soluzione Es. 139. Nel Teor. 17 si prendano $q_1 = \ell$, $q_2 = m$, $a_1 = a$, $a_2 = 1$. Vi sarà, dunque, un $\boldsymbol{a} \in \mathbb{N}$ tale che

$$a \;=\; (\boldsymbol{a} \,\%\, \ell)\;, \qquad 1 \;=\; (\boldsymbol{a} \,\%\, m)\;;$$

pertanto $\boldsymbol{a} \equiv a$ (**mod** ℓ) ed $\boldsymbol{a} \equiv 1$ (**mod** m). ⊣

Soluzione Es. 142. Partendo dalla prima formula si considerino, per ciascun $t \leqslant a$, valori $u_{t0}, \ldots, u_{tk}$ soddisfacenti la condizione $\forall\, z \leqslant y\, \exists\, v_1 \cdots \exists\, v_\ell \;\; P = Q$; si fissi poi, per ciascun $j \leqslant k$, un $q_j > \max\{u_{0j}, \ldots, u_{aj}\}$, sí da poter applicare il Lemma 18 alla corrispondente sequenza $q_j, u_{0j}, \ldots, u_{aj}$. Otteniamo cosí numeri a_j tali che $u_{tj} = a_j \,\%\, \big(1 + (a+1)! \cdot q_j \cdot (t+1)\big)$, per $t = 0, \ldots, a$. Basta dunque, per soddisfare la seconda formula, porre $d_j = (a+1)!\; q_j$ per ogni j.

Quando vale la seconda formula, si determini (con riferimento ad a_j e d_j fissati) la $k+1$ upla dei valori $u_j = a_j \,\%\, \big(1 + (t+1)\, d_j\big)$ corrispondenti a ciascun $t \leqslant a$, in maniera da soddisfare $\forall\, z \leqslant y\, \exists\, v_1 \cdots \exists\, v_\ell \;\; P = Q$. ⊣

Riferimenti bibliografici

[DMR76] Martin Davis, Yuri Matijasevič, and Julia Robinson. Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution. In *Mathematical Developments Arising From Hilbert Problems*, volume 28 of *Proceedings of Symposia in Pure Mathematics*, pages 323–378, Providence, RI, 1976. American Mathematical Society.

[Goe31] Kurt Goedel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. Math. und Physik*, 38:173–198, 1931. "On formally undecidable propositions of Principia Mathematica and related systems I" in Solomon Feferman, ed., 1986. Kurt Gödel Collected works, Vol. I. Oxford University Press: 144-195.