Un insieme diofanteo universale e due costruzioni diagonali

Eugenio G. Omodeo

30 marzo 2022

Introduzione

Intuitivamente parlando, un insieme $\mathcal{S}$ è *elencabile* se esiste un procedimento di calcolo concreto (o 'effettivo', come spesso si dice) in grado di generarne in sequenza gli elementi. Qualche esempio: sono elencabili

(A) qualsiasi sottoinsieme finito di $\mathbb{N} \coloneqq \{0, 1, 2, 3, 4, \ldots\}$: l'insieme vuoto, l'insieme dei quadrati perfetti minori di 122, ecc. ecc.;

(B) l'insieme (infinito) di tutti i numeri primi;

(C) fissato un qualsiasi polinomio $P(\vec{x})$ a coefficienti interi in una o piú variabili, $\vec{x}$, l'insieme (a volte finito, a volte infinito) di tutti quei valori $\geqslant 0$ che $P(\vec{x})$ assume al variare delle $\vec{x}$ su valori in $\mathbb{Z} \coloneqq \{0, \pm 1, \pm 2, , \pm 3, \ldots\}$;[1]

(D) fissato un polinomio $P(\vec{x})$ come al punto (C), l'insieme (a volte vuoto a volte no, forse anche infinito), di tutte le sostituzioni $\vec{\boldsymbol{x}}$ per le quali risulta $P(\vec{\boldsymbol{x}}) = 0$, di valori tratti da $\mathbb{N}$ alle $\vec{x}$.

Fra questi esempi, (C) e (D) ci dicono che non conviene insistere che gli elementi di un insieme elencabile vengano generati in un particolare ordine o senza doppioni. Cosí evitiamo bizantinismi: del resto, non ha rilevanza matematica se nella rappresentazione di un insieme vi siano o no elementi ripetuti né importa che gli elementi siano disposti in un particolare ordine piuttosto che alla rinfusa.

Il fatto che gli elementi di un insieme $\mathcal{S}$ possano venir elencati non assicura, di per sé, che esista un procedimento in grado di rispondere a ogni domanda della forma "$e \in \mathcal{S}$?". In effetti, generando gli elementi di $\mathcal{S}$ alla

[1] Come ben espone [12], l'insieme (B) ricade come caso particolare nello schema (C).

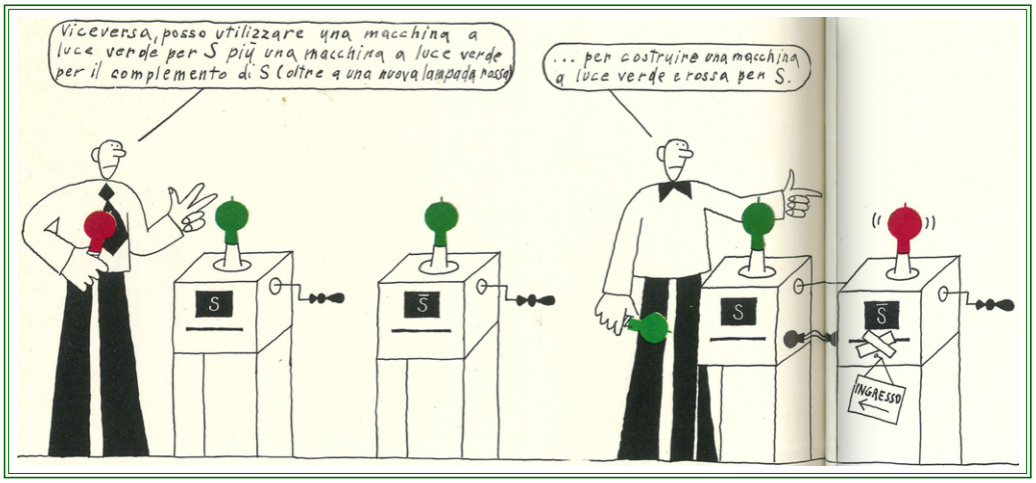


Figura 1: Come combinare due semi-decisori a formare un decisore (da [6])

rinfusa, prima o poi ci imbatteremo in e quando la risposta è affermativa; ma il non essersi imbattuti in e dopo che l'elencazione si è alquanto protratta, in genere non autorizza a escludere che proseguendo lo si possa incontrare. Come evidenzia la Fig. 1, un procedimento che dia correttamente tanto responsi affermativi che negativi esiste solo quando sono elencabili sia $\mathcal{S}$ che il suo complementare[2] $\overline{\mathcal{S}}$ (e in tal caso esiste).

Possediamo oggi molte caratterizzazioni di procedimento di calcolo effettivo ed esse sono equivalenti una all'altra, almeno per quanto riguarda la *calcolabilità* di una funzione (pur potendo differire per quanto attiene alla complessità algoritmica). A sottolineare lo scarto fra funzione calcolabile in senso intuitivo e funzione calcolabile ai sensi di un preciso linguaggio di specifica formale, ci riferiremo alla seconda come funzione *computabile*.

Alla luce della teoria delle funzioni computabili (vedi, ad es., [4] o [9]), gli insiemi elencabili possono venir caratterizzati in due modi:

(i) Un insieme $\Im \subseteq \mathbb{N}$ è **elencabile** se e solo se: o è vuoto oppure è l'insieme $\Im = \{f(\vec{\boldsymbol{x}}) : \vec{\boldsymbol{x}} \in \mathbb{N}^n\}$ di tutti i valori di una funzione $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ computabile e *totale* (i.e., f associa un valore a ogni $\vec{\boldsymbol{x}} \in \mathbb{N}^n$).

[2] In base al suo tipo, $\mathcal{S}$ avrà per complementare $\mathbb{N} \setminus \mathcal{S}$, $\mathbb{N}^m \setminus \mathcal{S}$, $(\bigcup_{m \in \mathbb{N}} \mathbb{N}^m) \setminus \mathcal{S}$, o altro.

(ii) Un insieme $\Re \subseteq \mathbb{N}^m$ è **elencabile** se e solo se esiste una funzione computabile *parziale* $g : \mathbb{N}^m \rightharpoonup \mathbb{N}$ tale che
$$\Re = \{\, \vec{\boldsymbol{x}} \in \mathbb{N}^m \mid \text{ la computazione di } g(\vec{\boldsymbol{x}}) \text{ fornisce un risultato} \,\}.$$

Può sembrare che la caratterizzazione (i) riguardi i sottoinsiemi di $\mathbb{N}$ e l'altra le relazioni m-adiche su $\mathbb{N}$; ma in realtà, grazie a una biiezione computabile che vedremo nel §1.4, $\mathbb{N}^m$ può venir assimilato a $\mathbb{N}$. Differenza piú notevole: al primo punto stiamo considerando la *multi-immagine* di una funzione f totale, nell'altro il *dominio* di una funzione g parziale. A ogni modo, si tratta di due caratterizzazioni equivalenti; benché la prima rifletta meglio la descrizione intuitiva suggerita all'inizio, spesso si adotta la seconda come definizione di insieme ENUMERABILE RICORSIVAMENTE (in breve '*r.e.*'). Si dice che un insieme r.e. $\mathcal{S} \subseteq \mathbb{N}$ è SEMPLICE se $\mathbb{N} \setminus \mathcal{S}$ è infinito ma non include alcun insieme r.e. infinito.

Fin qui ho accennato alla teoria della computabilità. Ora ci avvicineremo alla teoria dei numeri, cominciando da una terza caratterizzazione di insieme elencabile: quella di insieme *diofanteo* che sto per proporvi nel §1.1. Come Martin D. Davis aveva congetturato nel 1950 [3], gli insiemi diofantei coincidono con gli insiemi r.e., fatto che risultò dimostrato tramite due teoremi: quello di Davis-Putnam-Robinson del 1961 [8] e quello di Matiyasevich del 1970 [14]. Fatto noto come TEOREMA DPRM, dalle iniziali degli scopritori.[3]

Tramite la macchina universale di Turing [21], v. Fig. 2, si giunge presto a stabilire che esistono insiemi r.e. il cui complementare non è r.e.; pertanto, una volta stabilito che gli insiemi diofantei sono la stessa cosa che gli insiemi r.e., si potrà riferire quel risultato agli insiemi diofantei. Tuttavia, per mantenere una maggiore aderenza alla teoria dei numeri svincolandomi dalla teoria della computabilità, delineo in questa dispensa due dimostrazioni autonome del fatto che esistono sottoinsiemi diofantei Δ di $\mathbb{N}$ tali che $\mathbb{N} \setminus \Delta$ non è diofanteo (vedi §§2.2–2.3). Entrambe le dimostrazioni sfruttano un'equazione che ha un'*universalità* paragonabile a quella della macchina di Turing; entrambe si servono di tale equazione per un tipo di costruzione (risalente per lo meno a George F. L. Ph. Cantor) che va sotto il nome di *metodo diagonale*. La seconda costruzione produce un insieme diofanteo *semplice*.

[3] Grazie al primo dei due (teorema DPR), sappiamo che gli insiemi diofantei esponenziali coincidono con gli insiemi r.e.; grazie all'altro—quello di Matiyasevich—, che gli insiemi diofantei polinomiali coincidono con gli insiemi diofantei *esponenziali* (v. Appendice A).

Una volta specificato, tramite un'equazione diofantea universale, un insieme diofanteo a complementare non elencabile, si ottiene subito l'indecidibilità del 10º problema di Hilbert — come chiarirò nelle conclusioni.

1 Prerequisiti

1.1 Insiemi e relazioni diofantei

Definizione 1. *Si dice che una relazione* $\mathcal{D} \subseteq \mathbb{N}^m$ *è* DIOFANTEA *(di* dimensione $m \in \mathbb{N}$*) se esistono un* $t \in \mathbb{N}$ *e un polinomio*

$$D \in \mathbb{Z}[a_1, \ldots, a_m, x_{m+1}, \ldots, x_{m+t}]$$

a coefficienti interi nelle variabili distinte $\underbrace{a_1, \ldots, a_m}_{\text{parametri}}, \underbrace{x_{m+1}, \ldots, x_{m+t}}_{\text{incognite}}$ *tale che per ogni sequenza* $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \rangle \in \mathbb{N}^m$ *sussista la seguente condizione necessaria e sufficiente affinché* $\mathcal{D}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$*, viz* $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \rangle \in \mathcal{D}$ *:*

$$\mathcal{D}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m) \iff \left\{ \begin{array}{r} \text{l'equazione } D(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m, x_{m+1}, \ldots, x_{m+t}) = 0 \\ \text{ammette almeno una soluzione in } \mathbb{N}\,. \end{array} \right.$$

Quando $t = 0$*, una tale* $\mathcal{D}$ *si chiama* RELAZIONE POLINOMIALE*; quando* $m = 1$ *(e* $t \geqslant 0$*), si dice che essa è un* INSIEME DIOFANTEO. ⊣

Banalmente, le relazioni diofantee di dimensione $m = 0$ sono i bit $\emptyset$ e $\{\emptyset\}$.

Esempio tipico di relazione diofantea è quello in cui $\mathcal{D}$ è il grafo di una funzione $\mathcal{F}$ da un sottoinsieme di $\mathbb{N}^n$ in $\mathbb{N}$, specificabile come

$$\mathcal{F}(a_1, \ldots, a_n) = b \iff \exists\, y_1 \cdots \exists\, y_t\ \varphi(\overbrace{\underbrace{a_1, \ldots, a_n, b}_{\text{parametri}}, \underbrace{y_1, \ldots, y_t}_{\text{incognite}}}^{\text{variabili a due a due distinte}})\,, \qquad (\dagger)$$

per qualche formula φ che involge solo:

- variabili, includenti (come variabili libere) quelle mostrate,
- costanti intere positive,
- addizione, moltiplicazione, elevamento a costante intera positiva,
- i connettivi logici $=$, $\&$, $\vee$, $\exists\,\nu$. (Notare l'*assenza* di $\neg$, $\Rightarrow$, $\iff$).

L'Appendice A mostra diversi esempi di relazione diofantea.

1.2 L'abbinamento di Cantor

I numeri TRIANGOLARI sono, per definizione, quelli che risultano da una somma $1 + \cdots + m$ con $m \in \mathbb{N}$. Posto per brevità $T_m := 1 + \cdots + m$, avremo banalmente che $2 \cdot T_m = m \cdot (m+1)$ e potremo dunque esprimere il classico abbinamento biunivoco di Cantor da $\mathbb{N}^2$ a $\mathbb{N}$ come quella funzione $\mathtt{c}(i,j)$ che codifica la coppia $\langle i\,,\ j \rangle$ tramite il numero k per cui vale $2 \cdot k = 2 \cdot T_{i+j} + 2 \cdot i$ (eccoci imbattuti in una relazione polinomiale triadica!); dunque $2 \cdot \mathtt{c}(i,j) = (i+j) \cdot (i+j+1) + 2 \cdot i$, o piú in breve $2 \cdot \mathtt{c}(i,j) \;=\; (i+j)^2 + 3 \cdot i + j$.

In rappresentazione tabellare (cfr. [18, p. 78]):

	$\mathtt{c}(i,j)$	0	1	2	3	4	...
	0	0	1	3	6	10	...
	1	2	4	7	11	⋱	
i	2	5	8	12	⋱		
	3	9	13	⋱			
	4	14	⋱				
	⋮	⋱	⋱				

(j sopra la colonna 0)

ed inoltre, indicando con $\mathtt{l}(k)$ ed $\mathtt{r}(k)$ le due proiezioni della $\mathtt{c}(i,j)$:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...
$\mathtt{l}(k)$	0	0	1	0	1	2	0	1	2	3	0	1	2	3	4	0	...
$\mathtt{r}(k)$	0	1	0	2	1	0	3	2	1	0	4	3	2	1	0	5	...

Al pari di $\mathtt{c}(i,j)$, le sue proiezioni sono diofantee, in quanto

$$\begin{aligned} \mathtt{l}(k) = i \quad &\Longleftrightarrow \quad \exists\, j\, [\, 2 \cdot k = (i+j)^2 + 3 \cdot i + j\,]\,, \\ \mathtt{r}(k) = j \quad &\Longleftrightarrow \quad \exists\, i\, [\, 2 \cdot k = (i+j)^2 + 3 \cdot i + j\,]\,, \end{aligned}$$

o anche

$$\begin{aligned} \mathtt{l}(k) = i \quad &\Longleftrightarrow \quad \exists\, j \leqslant k\, [\, 2 \cdot k = (i+j)^2 + 3 \cdot i + j\,]\,, \\ \mathtt{r}(k) = j \quad &\Longleftrightarrow \quad \exists\, i \leqslant k\, [\, 2 \cdot k = (i+j)^2 + 3 \cdot i + j\,]\,. \end{aligned}$$

Esercizio 1. *Mostrare che* $\mathtt{l}(k) = i$ *&* $\mathtt{r}(k) = j$ *vale se e solo se* $i = k - w \cdot (w+1)/2$ *&* $j = w \cdot (w+3)/2 - k$, *ove—indicando con 'a ÷ b' il quoziente intero* $\lfloor \frac{a}{b} \rfloor$*—si ponga* $w = \big(-1 + \sqrt{1 + 8 \cdot k}\,\big) \div 2$. ⊣

1.3 Indicizzazione delle equazioni diofantee

Senza perdita di generalità,[4] possiamo considerare come equazioni diofantee tutte e sole le equazioni della forma $P = Q$, dove P e Q sono espressioni costruite a partire dalla costante 1 e dalle variabili $x_0\,,\ x_1\,,\ x_2\,,\ \ldots$ tramite gli operatori '$+$' e '$\cdot$' di somma e prodotto. Formiamo una successione $\boldsymbol{D}_0\,,\ \boldsymbol{D}_1\,,\ \boldsymbol{D}_2\,,\ldots$ in cui ogni espressione di tale tipo compare una e una sola volta, stabilendo che quando $i, j, k \in \mathbb{N}$ e $\mathsf{c}(i,j) = k$:

$$\begin{aligned} \boldsymbol{D}_{3\,k} &= \begin{cases} 1 & \text{se} \quad k = 0\,, \\ x_{k-1} & \text{altrimenti}\,, \end{cases} \\ \boldsymbol{D}_{3\,k+1} &= \boldsymbol{D}_i + \boldsymbol{D}_j\,, \\ \boldsymbol{D}_{3\,k+2} &= \boldsymbol{D}_i \cdot \boldsymbol{D}_j\,. \end{aligned}$$

La successione $\boldsymbol{D}_0\,,\ \boldsymbol{D}_1\,,\ \boldsymbol{D}_2\,,\ \ldots$ si sviluppa dunque cosí:

$$\begin{array}{rrrrrr} 1\,, & 1+1\,, & 1\cdot 1\,, & x_0\,, & 1+(1+1)\,, & 1\cdot(1+1)\,, \quad x_1\,, \\ (1+1)+1\,, & (1+1)\cdot 1\,, & x_2\,, & 1+(1\cdot 1)\,, & 1\cdot(1\cdot 1)\,, & x_3\,, \\ (1+1)+(1+1)\,, & (1+1)\cdot(1+1)\,, & x_4\,, & (1\cdot 1)+1\,, & (1\cdot 1)\cdot 1\,, & x_5\,, \\ 1+x_0\,, & 1\cdot x_0\,, & x_6\,, & (1+1)+(1\cdot 1)\,, & (1+1)\cdot(1\cdot 1)\,, & x_7\,, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

A questo punto viene naturale codificare l'equazione $\boldsymbol{D}_i = \boldsymbol{D}_j$ con il numero $\mathsf{c}(i,j)$; ciò facendo, abbiamo istituito una corrispondenza biunivoca fra $\mathbb{N}$ e l'insieme delle equazioni diofantee — equazioni da risolversi in $\mathbb{N}$.

Esempio 2. *Il numero 316664 codifica l'equazione* $x_1 \cdot x_1 = x_2 + x_2$. ⊣

Esercizio 3. *Mostrare che in* $\boldsymbol{D}_h$ *non compare alcuna variabile* x_k *il cui pedice* k *superi* h. ⊣

1.4 Codifica cantoriana delle tuple

In questa dispensa chiamiamo TUPLE le sequenze di qualsiasi lunghezza finita prefissata ℓ: quando, in particolare, $\ell = 2, 3, 4, 5$, le chiamiamo anche *coppie*, *terne*, *quaterne*, *cinquine*; per uniformità, quando vogliamo evidenziare la lunghezza ℓ delle tuple sotto esame, le chiamiamo ℓ-UPLE. Per sequenze finite di lunghezza non prefissata, impieghiamo il nome LISTE anziché 'tuple'.

Reiterando l'abbinamento di Cantor possiamo, per ogni $\ell > 0$, porre in corrispondenza biunivoca $\mathsf{c}_\ell(a_1, \ldots, a_\ell)$ con $\mathbb{N}$ l'insieme $\mathbb{N}^\ell$ delle ℓ-uple di

[4] Nella formulazione (†), al §1.1, abbiamo cercato di aumentare la comodità espressiva; ma qui, per tutt'altro obiettivo, ci conviene irrigidire la sintassi delle specifiche diofantee.

naturali; ecco come:

$$\begin{aligned} \mathsf{c}_1(a_1) &\coloneqq a_1\,, \\ \mathsf{c}_{m+2}(a_1,\ldots,a_{m+2}) &\coloneqq \mathsf{c}_{m+1}\big(a_1,\ldots,a_m,\mathsf{c}(a_{m+1},a_{m+2})\big)\,. \end{aligned}$$

Un'induzione mostra che il grafo di ciascuna di queste funzioni c_ℓ è diofanteo.[5]

1.5 Gödelizzazione di sequenze

Due tecniche di codifica delle liste di lunghezza varia vennero impiegate da Kurt Gödel nel suo epocale articolo del 1931 sugli enunciati indecidibili dell'aritmetica [10]. Delle due, la piú conosciuta poggia direttamente sul teorema fondamentale dell'aritmetica: sfruttando la successione dei numeri primi,

$$\langle \mathsf{p}_1,\mathsf{p}_2,\mathsf{p}_3,\mathsf{p}_4,\mathsf{p}_5,\mathsf{p}_6,\mathsf{p}_7,\mathsf{p}_8,\ldots\rangle \;\coloneqq\; \langle 2,3,5,7,11,13,17,19,\ldots\rangle\;,$$

si serve del prodotto $\prod_{i=1}^{\ell}\mathsf{p}_i^{e_i}$ per rappresentare la lista $\langle e_1,\ldots,e_\ell\rangle$. Ciò istituisce una suriezione da $\bigcup_{\ell\,\in\,\mathbb{N}}\mathbb{N}^\ell$ a $\mathbb{N}$; da un'immagine potremo risalire alla lista codificata solo se ne conosciamo la lunghezza ℓ, poiché tutte le liste di forma $\langle e_1,\ldots,e_\ell,0,\ldots,0\rangle$ hanno lo stesso numero.

L'altra tecnica introdotta da Gödel rappresenta una lista

$$\langle e_1,\ldots,e_\ell\rangle \qquad \text{di arbitraria lunghezza } \ell$$

tramite una qualsiasi delle infinite terne $\langle p,q,\ell\rangle\in\mathbb{N}^3$ che soddisfano:[6]

$$\begin{aligned} e_h &= p \,\%\, (h\,q+1)\,, && \text{per } h=1,\ldots,\ell; \\ q &\equiv 0 \mod \ell!\,, && q \text{ grande abbastanza perché} \\ & && e_h < h\,q+1 \text{ per } h=1,\ldots,\ell\,. \end{aligned}$$

L'esistenza di tali codifiche, per $\ell>0$, ci è assicurata da un corollario del ben noto teorema cinese dei resti (v. Appendice C). La 0-upla, banalmente, si rappresenta tramite qualsiasi terna $\langle p,q,0\rangle$ con $p,q\in\mathbb{N}$.

In quest'ottica gödeliana, possiamo liberalmente accettare che *ogni* terna su $\mathbb{N}$ codifichi una lista di naturali (vedi [15, pp. 42–43]):

$$\langle p,q,\ell\rangle \quad \text{codifica} \quad \langle (p\,\%\,(h\,q+1)) : h=1,\ldots,\ell\rangle\;.$$

[5] Ad es., per c_3 avremo: $8\,t = 4\,i^2+((j+k)^2+3\,j+k)^2+(4\,i+2)((j+k)^2+3\,j+k)+12\,i$.

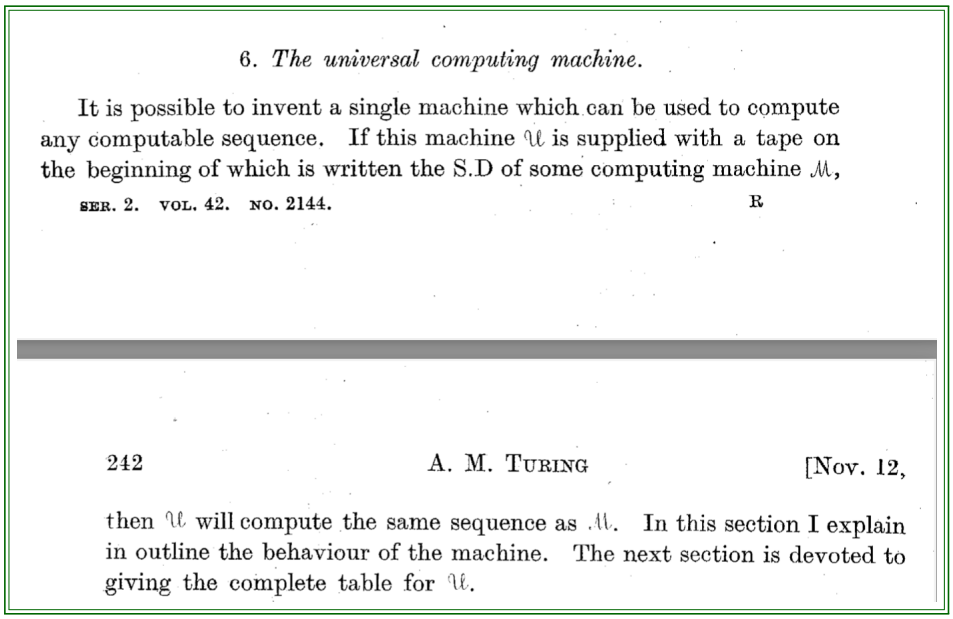
[6] Indichiamo con $h\,\%\,k$ il resto della divisione intera di h per k, ove $h,k\in\mathbb{N}$ e $k\neq 0$.

L'estrazione della $(h+1)$-esima voce di una lista codificata sarà dunque, per $h = 0, \ldots, \ell - 1$:

$$\texttt{gEl}(p, q, h) \coloneqq p \,\%\, \big((h+1)\, q + 1\big).$$

Esercizio 4. *Mostrare la coprimalità* $\ell!\, i\, r + 1 \perp \ell!\, j\, r + 1$ *ove* $1 \leqslant j < i \leqslant \ell + 1$*, per qualsiasi* $r > 0$. (Soluzione: Vedi Lemma 7 in Appendice C). ⊣

2 Un'equazione diofantea universale



6. *The universal computing machine.*

It is possible to invent a single machine which can be used to compute any computable sequence. If this machine $\mathfrak{U}$ is supplied with a tape on the beginning of which is written the S.D of some computing machine $\mathfrak{M}$,

SER. 2. VOL. 42. NO. 2144. R

242 A. M. TURING [Nov. 12,

then $\mathfrak{U}$ will compute the same sequence as $\mathfrak{M}$. In this section I explain in outline the behaviour of the machine. The next section is devoted to giving the complete table for $\mathfrak{U}$.

Figura 2: La macchina universale di Turing [21] evolverà in un'equazione

2.1 Sequenze conformi all'indicizzazione dei polinomi

È utile specificare la relazione $\texttt{Conf}(p, q, \ell)$ formata dalle terne $\langle p\,,\ q\,,\ \ell\rangle$ codificanti liste $\langle e_1\,, \ldots\,, e_\ell\rangle$ che per opportuni valori $\boldsymbol{x}$ delle variabili x soddisfano

il requisito $e_{h+1} = \boldsymbol{D}_h(\,\boldsymbol{x}_0\,,\,\boldsymbol{x}_1\,,\,\boldsymbol{x}_2\,,\ldots\,,\,\boldsymbol{x}_h\,)$ per $h = 0, \ldots, \ell - 1$:

$$\begin{aligned}\mathtt{Conf}(p,q,\ell) \;\coloneqq\; & \mathtt{gEl}(p,q,0) = 1 \;\&\; \boxed{\forall\, h < \ell} \;\exists\, i\,\exists\, j\,\exists\, k\Big[2\cdot k = 2\cdot \mathtt{c}(i,j) \;\&\\ & \big[\, h = 3\cdot k \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vee\\ & \big[h = 3\cdot k + 1 \;\&\; \mathtt{gEl}(p,q,h) = \mathtt{gEl}(p,q,i) + \mathtt{gEl}(p,q,j)\big] \vee\\ & \big[h = 3\cdot k + 2 \;\&\; \mathtt{gEl}(p,q,h) = \mathtt{gEl}(p,q,i)\cdot \mathtt{gEl}(p,q,j)\big]\big]\Big]\,.\end{aligned}$$

A tutta prima non è palese che questa relazione sia diofantea (su questo getterà luce l'Appendice B); contentiamoci per ora di osservare che è tale la relazione nei parametri p, q, h definita dalla formula

$$\begin{aligned}& \exists\, i\,\exists\, j\,\exists\, k\Big[2\cdot k = 2\cdot \mathtt{c}(i,j) \;\&\\ & \big[\, h = 3\cdot k \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vee\\ & \big[h = 3\cdot k + 1 \;\&\; \mathtt{gEl}(p,q,h) = \mathtt{gEl}(p,q,i) + \mathtt{gEl}(p,q,j)\big] \vee\\ & \big[h = 3\cdot k + 2 \;\&\; \mathtt{gEl}(p,q,h) = \mathtt{gEl}(p,q,i)\cdot \mathtt{gEl}(p,q,j)\big]\big]\Big]\,.\end{aligned} \qquad (\boldsymbol{\psi_h})$$

Per quanto riguarda il quantificatore universale limitato che compare nella specifica di `Conf`, è illusorio volerlo depotenziare scrivendo che

$$\mathtt{Conf}(p,q,\ell) \;\iff\; \mathtt{gEl}(p,q,0) = 1 \;\&\; \underbrace{(\boldsymbol{\psi_0}) \;\&\; \cdots \;\&\; (\boldsymbol{\psi_{\ell-1}})}_{\ell \text{ congiunti}}\,;$$

una congiunzione come questa, infatti, non è direttamente riscrivibile in termini polinomiali, non avendo un numero di congiunti costante bensí variabile.

2.2 Equazione diofantea universale e diagonalizzazione

L'equazione diofantea codificata dal numero k, ossia la $\boldsymbol{D}_{\mathtt{l}(k)} = \boldsymbol{D}_{\mathtt{r}(k)}$, ammette soluzione per $x_0 = a$ se e solo se

$$\begin{aligned}\exists\, p\,\exists\, q\,\exists\, \ell\,\exists\, i\,\exists\, j\Big[&\mathtt{Conf}(p,q,\ell) \;\&\; \mathtt{gEl}(p,q,3) = a \;\&\; \mathtt{c}(i,j) = k \;\&\\ &\ell > i \;\;\&\;\; \ell > j \;\&\; \mathtt{gEl}(p,q,i) = \mathtt{gEl}(p,q,j)\Big].\end{aligned} \qquad (\ddagger)$$

Pertanto, una volta che sia dimostrato (alla luce dell'Appendice B e del teorema di Matiyasevich) che

quando $\mathcal{D}(a_0, \ldots, a_m)$ è relazione diofantea, è tale anche la relazione definita dalla formula

$$\forall\, y < a_m\ \mathcal{D}(a_0, \ldots, a_{m-1}, y)\,,$$

otterremo che:

- la relazione definita dalla formula $\texttt{Conf}(p, q, \ell)$ è diofantea;
- la relazione $\mathcal{U}(a, k)$ definita dalla formula (‡) è diofantea, pertanto
- l'equazione diofantea $\texttt{U}(a, k, y_1, \ldots, y_t) = 0$ in cui è riscrivibile la (‡) è UNIVERSALE.

Il senso dell'ultima affermazione è che

per ogni insieme diofanteo $\mathcal{D}(a)$, è possibile impostare la variabile k a un valore $\boldsymbol{k}$ in modo da far valere, per qualsiasi naturale $\boldsymbol{a}$:

$$\mathcal{D}(\boldsymbol{a}) \iff \exists\, y_1\ \cdots\ \exists\, y_t\ \texttt{U}(\boldsymbol{a}, \boldsymbol{k}, y_1, \ldots, y_t) = 0\ .$$

Basta, in effetti, impostare k al valore $\texttt{c}(i, j)$ di un'equazione $\boldsymbol{D}_i = \boldsymbol{D}_j$ definente $\mathcal{D}$ per rendere vera, sui numeri naturali,

$$\mathcal{D} \;=\; \left\{\, x_0 \mid \exists\, x_1 \cdots \exists\, x_k\ \boldsymbol{D}_{\texttt{l}(k)}\,(x_0, x_1, \ldots, x_k) = \boldsymbol{D}_{\texttt{r}(k)}\,(x_0, x_1, \ldots, x_k) \right\}$$

e dunque far sí che sia vera la biimplicazione voluta.[7] Anche del polinomio $\texttt{U}$ si dice che è UNIVERSALE.

Un semplice argomento diagonale ci dice che l'insieme

$$\overline{\boldsymbol{\Delta}} \;\coloneqq\; \{\, x_0 \in \mathbb{N} \mid \neg\, \mathcal{U}(x_0, x_0)\,\}$$

non può essere diofanteo: se lo fosse, esisterebbe un numero $\boldsymbol{d}$ tale che

$$\begin{aligned}
&\forall\, x_0 \left(\, \overline{\boldsymbol{\Delta}}(x_0) \iff \exists\, y_1\ \cdots\ \exists\, y_t\ \texttt{U}(x_0, \boldsymbol{d}, y_1, \ldots, y_t) = 0 \,\right)\\
\therefore\ &\forall\, x_0 \left(\, \overline{\boldsymbol{\Delta}}(x_0) \iff \mathcal{U}(x_0, \boldsymbol{d}) \,\right)\\
\therefore\ &\overline{\boldsymbol{\Delta}}(\boldsymbol{d}) \iff \mathcal{U}(\boldsymbol{d}, \boldsymbol{d})\\
\therefore\ &\neg\, \mathcal{U}(\boldsymbol{d}, \boldsymbol{d}) \iff \mathcal{U}(\boldsymbol{d}, \boldsymbol{d})\,,
\end{aligned}$$

[7] Si noti che mentre non tutte le variabili $x_0, x_1, \ldots, x_k$ figurano davvero in $\boldsymbol{D}_{\texttt{l}(k)} = \boldsymbol{D}_{\texttt{r}(k)}$, segue dalle maggiorazioni $k \geqslant \texttt{l}(k)$, $k \geqslant \texttt{r}(k)$ che variabili in piú non ve ne sono.

col che cadremmo in contraddizione. È diofantea, invece, la condizione $\exists\, y_1 \,\cdots\, \exists\, y_t \; \mathtt{U}(a, a, y_1, \ldots, y_t) = 0$ che specifica il complementare $\boldsymbol{\Delta}$ di $\overline{\boldsymbol{\Delta}}$.

Qual è il valore di t? Potremmo calcolarlo, ma precisarlo avrebbe un interesse marginale in quanto esistono, senza dubbio, altri polinomi diofantei universali, e potrebbero avere un numero d'incognite piú basso di quelle che compaiono nel nostro $\mathtt{U}$. Questione piú degna d'interesse è, caso mai: Quanto si può rendere piccolo—tramite una costruzione piú sofisticata di quella sú proposta—il numero d'incognite di un polinomio diofanteo universale? Ad oggi, i migliori risultati in tal senso si trovano nel lavoro [11] di James Jones, che cerca di ottimizzare non solo il numero di incognite, ma anche il grado — com'è intuibile, sono due criteri in conflitto uno con l'altro.

2.3 Una diagonalizzazione piú sofisticata

Complichiamo un po' la costruzione diagonale appena vista, per ottenere un insieme diofanteo $\boldsymbol{\nabla}$ il cui complementare $\overline{\boldsymbol{\nabla}} \coloneqq \mathbb{N} \setminus \boldsymbol{\nabla}$ differisce da qualsiasi insieme diofanteo $\mathcal{D}$ in quanto:

(1) se $\mathcal{D}$ è infinito, allora $\mathcal{D} \cap \boldsymbol{\nabla} \neq \emptyset$ (dunque $\overline{\boldsymbol{\nabla}}$ lascia fuori elementi di $\mathcal{D}$);

(2) $\overline{\boldsymbol{\nabla}}$ è infinito (pertanto, se $\mathcal{D}$ è finito, $\overline{\boldsymbol{\nabla}}$ ha elementi di cui $\mathcal{D}$ è privo).

Poniamo:

$$\begin{aligned}\boldsymbol{\nabla}(a) \;\coloneqq\; & \exists\, k\, \exists\, y\, \forall\, z \leqslant y\, \exists\, z_0\, \exists\, y_1 \cdots \exists\, y_t \Big[\mathtt{c}_{t+1}(z_0, y_1, \ldots, y_t) = z \;\;\&\\ & \big[\big(2 \cdot k < z_0 \;\&\, \mathtt{U}(z_0, k, y_1, \ldots, y_t) = 0\big) \iff \big(z = y \;\&\, z_0 = a\big)\big]\Big];\end{aligned}$$

dunque $\boldsymbol{\nabla}(\boldsymbol{a})$ vale se e solo se:

- c'è un valore $\boldsymbol{k} < \frac{\boldsymbol{a}}{2}$ per cui l'eq. $\mathtt{U}(\boldsymbol{a}, \boldsymbol{k}, y_1, \ldots, y_t) = 0$ ha soluzione;
- fra le soluzioni $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_t$ di $\mathtt{U}(\boldsymbol{a}, \boldsymbol{k}, y_1, \ldots, y_t) = 0$ ce n'è una tale che nessuno dei valori $\boldsymbol{z} = \mathtt{c}_{t+1}(\boldsymbol{z}_0, \boldsymbol{z}_1, \ldots, \boldsymbol{z}_t)$ per cui sono vere $2\,\boldsymbol{k} < \boldsymbol{z}_0$ e $\mathtt{U}(\boldsymbol{z}_0, \boldsymbol{k}, \boldsymbol{z}_1, \ldots, \boldsymbol{z}_t) = 0$ sia piú piccolo di $\boldsymbol{y} = \mathtt{c}_{t+1}(\boldsymbol{a}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_t)$.

Osserviamo che $\boldsymbol{\nabla}$ è un insieme diofanteo[8] se è vero l'assunto (tuttora da dimostrare) che le relazioni diofantee di qualsiasi dimensione positiva sono

[8] Un uso liberale del connettivo '$\iff$' non è accettabile nella specifica di relazioni diofantee; qui lo utilizziamo solo per brevità, cautelandoci che sapremmo riscrivere questa biimplicazione impiegando solo i connettivi $=, \neq, <, \leqslant, \;\&, \vee$. Quanto al quantificatore limitato $\forall\, z \leqslant y$, è facile riscriverlo in termini di $\forall\, z < y$ (e anche viceversa).

chiuse rispetto alla quantificazione universale limitata. Passando ora a considerare un generico insieme diofanteo $\mathcal{D}$, verifichiamo che le condizioni (1) e (2) sono soddisfatte: da ciò conseguirà la non diofanticità di $\overline{\boldsymbol{\nabla}}$.

Supponiamo dapprima che $\mathcal{D}$ sia infinito e fissiamo $\boldsymbol{k}$ in modo che l'equazione $\mathtt{U}(a, \boldsymbol{k}, y_1, \ldots, y_t) = 0$ definisca $\mathcal{D}(a)$. Fra le tuple $\langle a, y_1, \ldots, y_t\rangle$ per cui vale $a \in \mathcal{D}$ ed $a > 2\,\boldsymbol{k}$, scegliamo quella, $\langle \boldsymbol{a}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_t\rangle$, che ha il valore $\boldsymbol{y} = \mathtt{c}_{t+1}(a, y_1, \ldots, y_t)$ piú piccolo di tutte; avremo cosí che $\boldsymbol{a} \in \mathcal{D} \cap \boldsymbol{\nabla}$, in accordo con la (1).

Prendiamo poi in esame un insieme diofanteo $\mathcal{D}$ il cui numero ℓ di elementi sia finito. Ragionando per assurdo, ipotizziamo violata la condizione (2); allora ad ogni $a \in \overline{\mathcal{D}}$ deve corrispondere un k_a conforme alla specifica di $\boldsymbol{\nabla}(a)$ e ciò vale, dunque, per particolari $a_0, a_1, \ldots, a_\ell \in \{0, 1, \ldots, 2\,\ell\}$ a due a due diversi. Osserviamo che i naturali $k_{a_0}, \ldots, k_{a_\ell}$ sono anch'essi[9] in numero di $\ell + 1$, ma ciò è incompatibile con il soddisfacimento simultaneo delle $\ell + 1$ disuguaglianze $k_{a_i} < \frac{a_i}{2} < \ell$. Questa contraddizione ci dà la (2). ⊣

Conclusione

Riprendendo il filo del discorso avviato nell'introduzione, chiediamoci ora se possa esistere un algoritmo che, ricevendo una qualsiasi equazione diofantea, ci dica se essa ammette o no soluzione in $\mathbb{N}$. Indichiamo con $\mathcal{S}$ e con $\overline{\mathcal{S}}$ l'insieme delle equazioni cui spetta risposta affermativa e, rispettivamente, negativa: grazie all'indicizzazione delle equazioni esposta al §1.3, è lecito pensare che $\mathcal{S} \subseteq \mathbb{N}$ e che $\overline{\mathcal{S}} = \mathbb{N} \setminus \mathcal{S}$. Affermare che esiste un algoritmo in grado di rispondere correttamente, dato il numero k di un'equazione, se $k \in \mathcal{S}$ oppure no, equivale ad affermare che sono elencabili tanto $\mathcal{S}$ che $\overline{\mathcal{S}}$.

Però l'inesistenza di un tale algoritmo consegue dall'esistenza di un insieme diofanteo Δ di numeri naturali il cui complementare $\overline{\Delta} \coloneqq \mathbb{N} \setminus \Delta$ non è diofanteo: ecco in che modo procede l'argomentazione. In base alla definizione

[9] Supponendo che $\boldsymbol{\nabla}(\boldsymbol{a})\ \&\ \boldsymbol{\nabla}(\boldsymbol{a'})\ \&\ k_{\boldsymbol{a}} = k_{\boldsymbol{a'}} = \boldsymbol{k}$, dimostriamo come segue che $\boldsymbol{a} = \boldsymbol{a'}$. Indichiamo con $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_t$ la soluzione di $\mathtt{U}(\boldsymbol{a}, \boldsymbol{k}, y_1, \ldots, y_t) = 0$ che assicura la minimalità rispetto a $\boldsymbol{k}$ e associamo analogamente $\boldsymbol{y'}_1, \ldots, \boldsymbol{y'}_t$ ad $\boldsymbol{a'}$; allora, supponendo per assurdo che $\boldsymbol{a} \neq \boldsymbol{a'}$, avremmo che $\mathtt{c}_{t+1}(\boldsymbol{a}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_t) \neq \mathtt{c}_{t+1}(\boldsymbol{a'}, \boldsymbol{y'}_1, \ldots, \boldsymbol{y'}_t)$ con $2\,\boldsymbol{k} < \boldsymbol{a}\ \&\ 2\,\boldsymbol{k} < \boldsymbol{a'}$; perciò il membro sinistro di questa disuguaglianza dovrebbe minorare il destro e viceversa.

di diofanticità abbiamo, per qualche $D \in \mathbb{Z}[a, x_1, \ldots, x_t]$, che[10]

$$\Delta \;=\; \left\{ a \in \mathbb{N} \mid \begin{array}{l} \text{l'equazione } D(a, x_1, \ldots, x_t) = 0 \\ \text{ammette almeno una soluzione in } \mathbb{N} \end{array} \right\};$$

perciò, se l'algoritmo in questione esistesse, potremmo servircene per stabilire, di qualsiasi dato $a \in \mathbb{N}$, se a appartenga a Δ oppure no. Sarebbe, dunque, elencabile $\overline{\Delta}$; interviene qui, di contro, il teorema DPRM, in base al quale ogni insieme elencabile è diofanteo.

Riferimenti bibliografici

[1] James Crawford Abbott, editor. *The Chauvenet Papers,* vol. *2.* Math. Assoc. of America, 1978.

[2] Douglas M. Campbell and John C. Higgins, editors. *Mathematics: People, Problems, Results*, volume 2. Wadsworth International, Belmont, CA, 1984.

[3] M. Davis. *On the theory of recursive unsolvability.* PhD thesis, Princeton Univ., 1950.

[4] M. Davis. *Computability and Unsolvability.* McGraw-Hill, New York, 1958. Reprinted with an additional appendix, Dover 1983.

[5] M. Davis. Hilbert's tenth problem is unsolvable. *Amer. Math. Monthly*, 80(3):233–269, 1973. Reprinted with corrections in the Dover edition of *Computability and Unsolvability* [4, pp. 199–235].

[6] M. Davis and Reuben Hersh. Hilbert's 10th problem. *Scientific American*, 229:84–91, 1973. Reprinted in [1, pp. 555–571] and in [2, pp. 136–148].

[7] 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. Reprinted in [19, p. 269ff.].

[8] Martin Davis, Hilary Putnam, and Julia Robinson. The decision problem for exponential Diophantine equations. *Ann. of Math.,* 2nd *Series*, 74(3):425–436, 1961.

[9] Martin D. Davis, Ron Sigal, and Elaine J. Weyuker. *Computability, complexity, and languages - Fundamentals of theoretical computer science.* Computer Science ad scientific computing. Academic Press, 1994.

[10] Kurt Gödel. 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 Univ. Press: 144-195.

[10] Per entrambi gli insiemi $\boldsymbol{\Delta}$ ed $\boldsymbol{\nabla}$ visti piú su, un corrispondente D è, di fatto, noto.

[11] James P. Jones. Universal Diophantine equation. *The Journal of Symbolic Logic*, 47(3):549–571, 1982.

[12] 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.

[13] Ju. V. Matijasevič. Enumerable sets are Diophantine. *Soviet Mathematics. Doklady*, 11(3):354–358, 1970. (Translated from [14]).

[14] Yu. V. Matiyasevich. Diofantovost' perechislimykh mnozhestv. *Doklady Akademii Nauk SSSR*, 191(2):279–282, 1970. (Russian. Available in English translation as [13]; translation reprinted in [20, pp. 269–273]).

[15] Yuri Vladimirovich Matiyasevich. *Desyataya Problema Gilberta*. Fizmatlit, Moscow, 1993. English translation: *Hilbert's Tenth problem*. The MIT Press, Cambridge (MA) and London, 1993. French translation: *Le dixième Problème de Hilbert: son indécidabilité*, Masson, Paris Milan Barcelone, 1995. URL: http://logic.pdmi.ras.ru/∼yumat/H10Pbook/.

[16] M. Ram Murty and Fodden Brandon. *Hilbert's tenth problem. An Introduction to Logic, Number Theory, and Computability*, volume 88 of *Student mathematical library*. American Mathematical Society, Providence, RI, 2019.

[17] J. Robinson. Existential definability in arithmetic. *Transactions of the American Mathematical Society*, 72(3):437–449, 1952. Reprinted in [19, p. 47ff.].

[18] 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.

[19] 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.

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

[21] Alan Mathison Turing. On Computable Numbers, with an application to the Entscheidungsproblem. *Proc. London Math. Soc.*, 2(42):230–265, 1936. Correction, ibid., (43):44-546, 1937.

A Es. di relazioni diofantee (. . . esponenziali?)

Cominciamo con la specifica diofantea di alcune relazioni basilari tra numeri naturali (fra cui la divisibilità, '|', e i grafi delle operazioni '÷' e '%' di quoziente e resto):

$$\begin{array}{rcl} a \leqslant b & \coloneqq & \exists\, x\ b = a + x\,; \\ a < b & \coloneqq & \exists\, x\ b = a + x + 1\,; \\ a \mid b & \coloneqq & \exists\, q\ b = a \cdot q\,; \\ b \,\%\, a = r & \coloneqq & \exists\, q \left(a \cdot q + r = b \ \ \& \ \ r < a \right); \\ b \div a = q & \coloneqq & \exists\, r \left(a \cdot q + r = b \ \ \& \ \ r < a \right); \\ d \equiv r \mod p & \coloneqq & p \mid \pm(d - r)\,, \\ \text{i.e.,}\quad d \equiv r \mod p & \coloneqq & \exists\, q \left(p^2\, q^2 + 2\, d\, r = d^2 + r^2 \right). \end{array}$$

Dando poi per assodato—benché si tratti di un risultato tutt'altro che banale— che la relazione triadica $b^a = c$ è diofantea, passiamo alla specifica diofantea di altre importanti relazioni: fra di esse, il grafo del coefficiente binomiale e il grafo del fattoriale. Per sottolineare che nelle specifiche a seguire stiamo usando l'elevamento a potenza (con coefficiente variabile) come 'scorciatoia', le diremo specifiche diofantee *esponenziali*.

La Fig.3 evidenzia che 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 $\left((2^\ell + 1) + 1\right)^\ell = \sum_{i=0}^{\ell} \binom{\ell}{i} (2^\ell + 1)^i$. Quindi varrà $\binom{\ell}{i} = a$ se e solo se vi sono u, v, w, x, y tali che[11]

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

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 3: Riguardo alla specifica diofantea esponenziale dei coefficienti binomiali

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

Piú brevemente, possiamo richiedere che

$$a = \big(\big((u+1)^\ell \div u^i\big) \,\%\, u\big) \quad \& \quad u = 2^\ell + 1 \ .$$

Il seguente risultato, che origina da [17], mostra che il fattoriale ha un grafo diofanteo esponenziale; per una sua dimostrazione, rinvio il lettore a [5, pp. 250–251].

Lemma 1. *Vale*

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

(*ossia* $j! = r^j \div \binom{r}{j}$).[12]

La diofanticità esponenziale del fattoriale, unita alla proposizione che segue, comporta la diofanticità esponenziale del costrutto $\prod_{k=1}^{c}(a + b\,k)$, cfr. [8, p. 433]:

Lemma 2. *Dati* a, b, c, d *con* $b > 0$ *e* $c > 0$*, la relazione*

$$\prod_{k=1}^{c}(a + b\,k) \ = \ d$$

vale se e solo se esistono m, q, p *tali che*

$$m = b\,(a + b\,c)^c + 1 \ \ \& \ \ b\,q = a + m\,p \ \ \& \ \ d \equiv b^c\,c!\,\binom{q+c}{c} \mod m \ \ \& \ \ d < m\,.$$

Dimostrazione. (Da [16, pp.148–149]) Utile rilievo preliminare: Se $b\,q \equiv a \mod m$, allora —richiamando che $\binom{q+c}{c} = \frac{(q+c)!}{c!\,(q+c-c)!}$:

$$\begin{aligned} \prod_{k=1}^{c}(a + b\,k) \ &\equiv \ \prod_{k=1}^{c}(b\,q + b\,k) \\ &\equiv \ b^c\ \prod_{k=1}^{c}(\ q + \ k\ ) \ = \ b^c\,c!\,\tbinom{q+c}{c} \qquad \mod m\,. \end{aligned}$$

('$\Rightarrow$') Supponendo che m, q, p soddisfino i vincoli indicati, otteniamo

$$m > (a + b\,c)^c \geqslant \prod_{k=1}^{c}(a + b\,k) \equiv b^c\,c!\,\binom{q+c}{c} \mod m\,,$$

[12] Matiyasevich [15, p. 46] "ritocca" questo enunciato dimostrando che $j! = r^j \div \binom{r}{j}$ vale per $r \geqslant (j+1)^{j+2}$. Un'altra variante ancora di questo enunciato, grazie alla quale si ha che

$$\boxed{\ j! \ = \ \big((2\,j)^{j\,j}\big) \div \binom{(2\,j)^{j\,j}}{j}\ }\,,$$

viene dimostrata in [16, pp. 145–147 e p. 166].

donde $d = \prod_{k=1}^{c}(a + b\,k)$ come voluto, poiché vale anche

$$m > d \equiv b^c\, c! \binom{q+c}{c} \mod m\,.$$

('$\Leftarrow$') Supponendo che $d = \prod_{k=1}^{c}(a + b\,k)$ e assegnando ad m il valore richiesto dal primo vincolo, $m > d$ seguirà da $m > (a + b\,c)^c$; avremo inoltre $m \perp b$ e dunque potremo trovare (v. sotto, Esercizio 5) $q, p \in \mathbb{N}$ tali che $q\,b - a = p\,m$ e dunque $b\,q \equiv a \mod m$. Anche la congruenza riguardante d risulterà soddisfatta, per il rilievo preliminare. ⊣

Esercizio 5 (Cfr. [16, p. 44])**.** *Dimostrare che quando a, b sono interi positivi:*

- *l'equazione $a\,X + b\,Y = C$ nelle incognite X, Y ha soluzione in $\mathbb{Z}$ per tutti e soli quei valori interi del parametro C per i quali $\mathsf{MCD}\,(a, b) \mid C$;*
- *lo schema $X = X_0 + (b/d)\,T$, $Y = Y_0 - (a/d)\,T$ genera, al variare di T in $\mathbb{Z}$, tutte le soluzioni intere di detta equazione da qualsiasi coppia X_0, Y_0 che la risolva.* ⊣

B Diofanticità e quantificazione limitata

La dimostrazione che la famiglia delle relazioni diofantee è chiusa rispetto alla quantificazione universale limitata può essere sviluppata in modi molto diversi (vedi [15, Cap.6]); quella che qui sotto riprendiamo dalla recente monografia [16] origina da [5, pp. 252–256], che a sua volta origina da [8, pp. 433–435].

Lemma 3. *A ogni polinomio diofanteo $P(h\,,\,k\,,\,x_1\,,\ldots,\,x_n\,,\,y_1\,,\ldots,\,y_m)$ corrisponde almeno un polinomio $Q(h\,,\,u\,,\,x_1\,,\ldots,\,x_n)$ tale che:*

(a) $Q(h\,,\,u\,,\,x_1\,,\ldots,\,x_n) > u$;

(b) $Q(h\,,\,u\,,\,x_1\,,\ldots,\,x_n) > h$;

(c) *quando $k \leqslant h$ ed $y_1\,,\ldots,\,y_m \leqslant u$, si ha che*

$$Q(h\,,\,u\,,\,x_1\,,\ldots,\,x_n) \quad \geqslant \quad |P(h\,,\,k\,,\,x_1\,,\ldots,\,x_n\,,\,y_1\,,\ldots,\,y_m)|\ .$$

Dimostrazione. (Da [16, p. 154])**.** Per trasformare P in un Q conforme alle condizioni:

- sostituire a ogni coefficiente di P il suo valore assoluto;
- sostituire: $k \rightsquigarrow h$ ed $y_1 \rightsquigarrow u\,,\ldots,\,y_m \rightsquigarrow u$;
- sommare $u + h + 1$ al polinomio fin qui ottenuto. ⊣

Lemma 4. *Se P e Q sono correlati come nel Lemma 3, allora dati $h, u, x_1, \ldots, x_n$ varrà*

$$\forall\, k \leqslant h\, \exists\, y_1 \leqslant u \cdots \exists\, y_m \leqslant u \quad P(h\,,\,k\,,\,x_1\,,\ldots,\,x_n\,,\,y_1\,,\ldots,\,y_m) \quad = \quad 0$$

se e solo se esistono c, t, $a_1\,,\ldots,\,a_m$ tali che

(1) $1+(c+1)\,t = \prod_{k=0}^{h}\big(1+(k+1)\,t\big)$;

(2) $t = Q(h\,,\,u\,,\,x_1\,,\ldots,\,x_n)\,!$;

(3) $1+(c+1)\,t \;\Big|\; \prod_{j=0}^{u}(a_i-j)$, *per* $i=1,\ldots,m$;

(4) $P(h\,,\,c\,,\,x_1\,,\ldots,\,x_n\,,\,a_1\,,\ldots,\,a_m) \;\equiv\; 0 \mod 1+(c+1)\,t$.

Dimostrazione. (Da [16, pp. 150–153]).

('⇒'): Supponendo vi siano, per $k=0,1,\ldots,h$, dei numeri $y_{k,i}\leqslant u$ tali che

$$P(h\,,\,k\,,\,x_1\,,\ldots,\,x_n\,,\,y_{k,1}\,,\ldots,\,y_{k,m}) \;=\; 0\,,$$

poniamo $t = Q(h\,,\,u\,,\,x_1\,,\ldots,\,x_n)\,!$ come richiede la (2). Dato che $\prod_{k=0}^{h}\big(1+(k+1)\,t\big)\equiv 1 \mod t$ e che $t\geqslant 1$, c'è un $c\geqslant 0$ per cui vale la (1). I numeri $1+(k+1)\,t$ risultano, al variare di k in $\{0,1,\ldots,h\}$, a due a due coprimi; perciò ben si prestano alla codifica, via teorema cinese dei resti, delle $(h+1)$-uple che abbiano componenti minori di t. In particolare esistono valori $a_1,\ldots,a_m$ codificanti le tuple $\langle y_{0,1}\,,\ldots,y_{h,1}\rangle\;\ldots,\;\langle y_{0,m}\,,\ldots,y_{h,m}\rangle$, nel senso che (cfr. §1.5):

$$y_{k,i} = a_i \;\%\; \big(1+(k+1)\,t\big)$$

vale per ogni k ed ogni i. Non è problematico esigere che $a_i > u$ per ogni i, in quanto sommare ad a_i la quantità positiva $\prod_{k=0}^{h}\big(1+(k+1)\,t\big)$ non influisce sulle congruenze. La (1) ci dà che $1+(k+1)\,t \mid 1+(c+1)\,t$ da cui scende la congruenza $(k-c)\,t\equiv 0 \mod \big(1+(k+1)\,t\big)$; da qui, considerato che $\mathsf{MCD}\,(t,1+(k+1)\,t)=1$, otteniamo $k\equiv c \mod \big(1+(k+1)\,t\big)$, cosicché

$$\begin{aligned} P(h\,,\,c\,,\,x_1\,,\ldots,\,x_n\,,\,a_1\,,\ldots,\,a_m) \;&\equiv \\ P(h\,,\,k\,,\,x_1\,,\ldots,\,x_n\,,\,y_{k,1}\,,\ldots,\,y_{k,m}) \;&\equiv\; 0 \mod 1+(k+1)\,t\,. \end{aligned}$$

Grazie alla coprimalità fra i numeri $1+(k+1)\,t$ e tenendo conto che ciascuno di loro divide $P(h\,,\,c\,,\,x_1\,,\ldots,\,x_n\,,\,a_1\,,\ldots,\,a_m)$, otteniamo che anche il loro prodotto divide $P(h\,,\,c\,,\,x_1\,,\ldots,\,x_n\,,\,a_1\,,\ldots,\,a_m)$, ossia la (4). Per concludere: dato che $0\leqslant y_{k,i}\leqslant u$, da $1+(k+1)\,t \mid a_i - y_{k,i}$ otteniamo che $1+(k+1)\,t \;\Big|\; \prod_{j=0}^{u}(a_i-j)$, donde la (3), tenendo di nuovo conto della coprimalità fra i numeri $1+(k+1)\,t$.

('⇐', solo un accenno): Supponendo soddisfatte le condizioni (1)–(4), associamo a ciascun $k\in\{0,\ldots,h\}$ un divisore primo p_k del numero $1+(k+1)\,t$; poniamo poi $y_{k,i} = a_i \;\%\; p_k$ per ogni k e per $i=1,\ldots,m$. Risulteranno allora soddisfatte tanto la disequazione $y_{k,i}\leqslant u$ che l'uguaglianza $P(h\,,\,k\,,\,x_1\,,\ldots,\,x_n\,,\,y_{k,1}\,,\ldots,\,y_{k,m})=0$, per ciascun k. ⊣

Teorema 5. *Se P e Q sono correlati come nel Lemma 3, allora dati $h,x_1,\ldots,x_n$ varrà*

$$\forall\, k\leqslant h\;\exists\, y_1\;\cdots\;\exists\, y_m \quad P(h\,,\,k\,,\,x_1\,,\ldots,\,x_n\,,\,y_1\,,\ldots,\,y_m) \;=\; 0$$

se e solo se esistono u, c, t, $a_1\,,\ldots,\,a_m$, $g_1\,,\ldots,\,g_m$, e tali che

(1) $e = 1+(c+1)\,t \;\;\&\;\; e = \prod_{k=0}^{h}\big(1+(k+1)\,t\big)$;

(2) $t = Q(h\,,\,u\,,\,x_1\,,\ldots,\,x_n)\,!$;

(3) $g_i + u = a_i \;\;\&\;\; e \;\Big|\; \prod_{j=0}^{u}(g_i + j)$, *per* $i = 1, \ldots, m$;

(4) $e \mid P(h\,,\, c\,,\, x_1\,, \ldots,\, x_n\,,\, a_1\,, \ldots,\, a_m)$.

Dimostrazione. (Da [16, pp. 153–155])**.** Per ricondursi al Lemma 4 basta osservare che

$$\begin{array}{rcl} \forall\, k \leqslant h\, \exists\, y_1 \cdots \exists\, y_m \quad P(h\,,\, k\,,\, x_1\,, \ldots,\, x_n\,,\, y_1\,, \ldots,\, y_m) & = & 0 \\ & \Longleftrightarrow & \\ \exists\, u\, \forall\, k \leqslant h\, \exists\, y_1 \leqslant u \cdots \exists\, y_m \leqslant u \quad P(h\,,\, k\,,\, x_1\,, \ldots,\, x_n\,,\, y_1\,, \ldots,\, y_m) & = & 0\,. \end{array}$$

In effetti, l'implicazione '$\Leftarrow$' è ovvia. Quanto alla '$\Rightarrow$', ragioniamo cosí: Supponendo vi siano, per $k = 0, 1, \ldots, h$, dei numeri $y_{k,i}$ tali che

$$P(h\,,\, k\,,\, x_1\,, \ldots,\, x_n\,,\, y_{k,1}\,, \ldots,\, y_{k,m}) \;=\; 0\,,$$

per soddisfare il conseguente si porrà $u = \max\left\{\, y_{k,i} : k \in \{0, \ldots, h\}\ ,\ i \in \{1, \ldots, m\}\,\right\}$.

(**Oss.:** Stiamo implicitamente richiedendo che la differenza $a_i - u$ sia un numero naturale g_i; pretesa legittima, alla luce della dimostrazione del Lemma 4.) ⊣

C 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." [7][13]

Teorema 6 (**Teorema cinese dei resti**)**.**

Se $q_0, q_1, \ldots, q_n, a_0, a_1, \ldots, a_n$ *sono interi tali che per* $i = 0, 1, \ldots, n$*:*

- 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 e un sol numero $\boldsymbol{a}$*,* $0 \leqslant \boldsymbol{a} < \prod_{i=0}^{n} q_i$*, tale che*

$$a_i \;=\; \boldsymbol{a} \,\%\, q_i\,, \qquad \textit{per } i = 0, 1, \ldots, n.$$

[13] Il [18] di quest'epigrafe si riferisce alla voce bibliografica indicata come [10] in questa dispensa.

Dimostrazione. Le $n+1$-uple distinte della forma

$$\langle (a \,\%\, q_0), \ldots, (a \,\%\, q_n) \rangle , \qquad \text{con } 0 \leqslant a < \textstyle\prod_{i=0}^{n} q_i,$$

sono, in tutto, esattamente $\prod_{i=0}^{n} q_i$—numero pari a quello delle n-uple $a_0, \ldots, a_n$ che soddisfano i vincoli $0 \leqslant a_i < q_i$. Questo perché quando a', a'' con $0 \leqslant a' \leqslant a'' < \prod_{i=0}^{n} q_i$ soddisfano le $(a' \,\%\, q_i) = (a'' \,\%\, q_i)$, cioè $q_i \mid a'' - a'$ per ogni i, la coprimalità fra q_i implica $\prod_{i=0}^{n} q_i \mid a'' - a'$, il che tiene solo se $a' = a''$. ⊣

Lemma 7 (Gödel, 1931)**.**

Se $q, a_0, a_1, \ldots, a_n$ sono interi tali che

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

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

$$a_i \quad = \quad \boldsymbol{a} \,\%\, \big(1 + n!\, q\, (i+1)\big), \qquad \textit{per } i = 0, 1, \ldots, n.$$

Dimostrazione. Posto $\boldsymbol{b} \ := \ n!\, q$, cosí che $(h+1)\,\boldsymbol{b} > a_h$ per $h = 0, \ldots, n$, onde poter ricorrere al Teor.6 ci basta mostrare la coprimalità $(i+1)\,\boldsymbol{b}+1 \perp (j+1)\,\boldsymbol{b}+1$ per $j < i \leqslant n$. In effetti, se esistesse un numero primo p tale che $p \mid (i+1)\,\boldsymbol{b}+1$ e $p \mid (j+1)\,\boldsymbol{b}+1$, dovremmo avere che $p \mid (i-j)\,\boldsymbol{b}$ mentre $p \nmid \boldsymbol{b}$; dunque $p \mid i - j$ dove $i - j < n$, ma allora $p \mid n!$ e pertanto $p \mid \boldsymbol{b}$, contraddizione. ⊣

Corollario 8. *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 7. ⊣

Esercizio 6. *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*

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