Appunti sul decimo problema di Hilbert

Eugenio G. Omodeo

18 marzo 2017

Indice

1 Formulazione del problema

In occasione del *Congresso internazionale dei matematici* a Parigi, l'8 agosto 1900, David Hilbert avanzò 23 problemi.[1] Il suo decimo problema (vedi Fig. 1) richiedeva di:

> **Determinare la risolubilità di un'equazione diofantea.**
>
> Data un'equazione diofantea in qualsiasi numero d'incognite e a coefficienti interi razionali: *Esporre un procedimento per mezzo del quale si possa stabilire, in un numero finito di operazioni, se l'equazione sia risolubile negli interi razionali.* [Hil00]

'Intero razionale' va inteso, semplicemente, come 'numero intero' (positivo, negativo, o nullo, vedi Fig. 2). Le equazioni di cui si parla sono polinomiali e i polinomi in questione sono chiamati DIOFANTEI come tributo al matematico alessandrino Diofanto. Cosí come non viene limitato il numero delle incognite, neppure viene posto un limite al grado dei polinomi. È verosimile che Hilbert contasse di ricavare da un algoritmo risolutivo riguardante le soluzioni intere un analogo algoritmo riguardante le soluzioni sui numeri razionali (v. sotto, § 1.3).

Hilbert

10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.

Eine Diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

Figura 1: Formulazione originaria del decimo problema di Hilbert.

Esempio 1. *L'equazione*

$$(X-Y-Z)^2 + (Y-Z-X)^2 + (Z-X-Y)^2 + (X^2-X) + (Y^2-Y) + (Z^2-Z) = 0$$

nelle tre incognite X, Y, Z ammette soluzioni intere? — E se sí, quante e quali?

R.: *C'è un'unica soluzione, la $X = Y = Z = 0$, in quanto dall'equazione discende che $\{X, Y, Z\} \subseteq \{0, 1\}$, $X = Y + Z$ ed $X \leqslant Y \leqslant Z \leqslant X$.*

[1] "Il giorno presente, che sta all'incontro tra secoli, mi sembra appropriato a una tale rassegna di problemi, in quanto il chiudersi di una grande epoca non solo invita a riesaminare il passato ma anche dirige i nostri pensieri al futuro sconosciuto." (Da [Hil00])

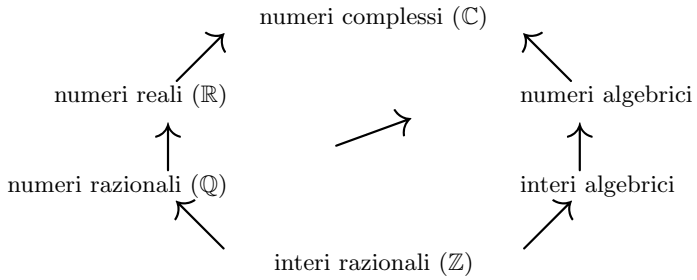


Figura 2: Relazioni d'inclusione fra le piú comuni nozioni di numero.

Nella formulazione del suo decimo problema, Hilbert non fa uso della parola *algoritmo*, oggi molto piú in voga che nel 1900;[2] ma è ben chiaro che quando richiede 'a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers',[3] il matematico di Gottinga si riferisce a quello che noi chiameremmo un *algoritmo decisionale*. Vale a dire: ricevendo P—uno qualsiasi degli infiniti polinomi a coefficienti interi, opportunamente rappresentato—, l'algoritmo dovrebbe dirci se l'equazione $P = 0$ ammetta *o no* soluzioni.

Esercizio 2. *Spiegate come un (ipotetico) algoritmo del tipo richiesto da Hilbert potrebbe venir trasformato in un procedimento che non solo stabilisca se l'equazione $P = 0$ abbia o no soluzioni, ma in caso affermativo ne fornisca una.*

Osservazione 3. *Come emerge da [Sko34], il 10° problema di Hilbert potrebbe essere riferito, senza perdita di generalità, a equazioni (di grado 4) della forma*

$$(U-1)^2 \quad + \quad \sum_{i=1}^{h}(V_i^2 - W_i)^2 \quad + \quad \sum_{j=1}^{k}(X_j + Y_j - Z_j)^2 \quad = \quad 0$$

(con h, k interi positivi), in cui le incognite sono U e le V_i, W_i, X_j, Y_j, Z_j—variabili non obbligatoriamente distinte una dall'altra.

Notazione 4. *Spesso, in ciò che segue, riscriviamo un'equazione polinomiale $P = 0$ nella forma $P_{\mathsf{sn}} = P_{\mathsf{dx}}$. Gli addendi del polinomio originario P saranno stati—tacitamente—distribuiti ai due lati dell'uguaglianza per non mettere in campo la sottrazione, né coefficienti negativi.*

1.1 Ammissibile una soluzione 'negativa' del X di Hilbert?

Pur aspettandosi che una tecnica per risolvere le equazioni diofantee sarebbe stata scoperta, Hilbert lasciava adito a un eventuale responso d'insolubilità:

[2] Va detto che all'epoca il concetto di algoritmo mancava di un'esplicitazione matematica in termini 'chiari e distinti', qual è emersa nei tre o quattro decenni successivi dal lavoro—per citare solo alcuni—di Alonzo Church, Kurt Gödel, Alan Mathison Turing ed Emil Leon Post.

[3] Da una trad. del 1902, dovuta a Mary Winston Newson e autorizzata dallo stesso Hilbert.

> " [· · ·] ogni problema matematico, precisato con cura, sarà suscettibile di una composizione esatta: o nella forma di un'effettiva risposta a quanto domandato; o tramite la dimostrazione che una sua soluzione è impossibile, cosicché ogni tentativo deve per forza fallire."
> *[Hil00]*

Va segnalata una profonda dissimmetria fra un'ipotetica soluzione positiva al X problema di Hilbert e un responso d'insolubilità algoritmica. Già in epoca pre-informatica era pacifico che la descrizione di un algoritmo decisionale dovesse improntarsi a estrema diligenza e cura del dettaglio—come, altrimenti, stabilire che i responsi sarebbero stati affidabili?—; ma la stesura dei procedimenti non doveva ancora sottostare a quel grado di formalizzazione—eccessivo, non di rado, anche per il gusto matematico—che contraddistingue i programmi per *computer*.

Per contro, dimostrare che *nessun* algoritmo può risolvere il compito del X problema di Hilbert, richiedeva che la nozione stessa di algoritmo fosse definita in assoluto rigore. È attorno al 1936–1937 che varie esplicitazioni matematiche della "*computabilità effettiva*" vengono riconosciute tra loro equivalenti e solo allora prende piede l'idea che esse catturino il concetto intuitivo di *calcolabilità*. L'ipotesi filosofica—oggi largamente condivisa—che le due nozioni, una formale l'altra no, si riflettano appieno una nell'altra è nota come *tesi di Church*, o *tesi di Church-Turing*, o *tesi di Turing-Church*.

L'aggancio dello studio della calcolabilità a un fermo fondamento matematico si rivela indispensabile proprio in relazione all'ambizioso *Entscheidungsproblem* (vedi sotto, § 1.4) sollevato da Hilbert assieme al suo allievo Wilhelm Friedrich Ackermann sul finire degli anni 1920, di cui il X problema già incorporava—senza che Hilbert potesse immaginarlo—le intrinseche difficoltà.

Negli anni 1930 Gödel ottiene formidabili risultati limitativi circa il metodo assiomatico, sulla scorta dei quali Church e Turing individuano sotto-problemi algoritmicamente insolubili dell'*Entscheidungsproblem*. Pochi anni dopo, Emil Post comincia a intravedere l'insolubilità del X problema di Hilbert e trasmette quest'attesa 'negativa' al suo allievo Martin David Davis.

"While I was still an undergraduate at City College in New York, I read my teacher E. L. Post's plaint that Hilbert's Tenth Problem "begs for an unsolvability proof" This was the beginning of my lifelong obsession with the problem." (Martin Davis, 1993)

(*Emil Leon Post*, 1897–1954)

Figura 3: Un *imprinting*, una fissazione.

Esercizio 5. *In [Dav68], Martin Davis congetturava che l'equazione*

$$9\,(X^2+7\,Y^2)^2-7\,(U^2+7\,V^2)^2 \;=\; 2$$

non avesse, sui numeri naturali*, altra soluzione che quella banale*

$$X \;=\; U \;=\; 1\,, \qquad Y \;=\; V \;=\; 0\,.$$

Esprimete questa congettura come un caso particolare del X problema di Hilbert.

1.2 Un'innocua 'semplificazione' del X di Hilbert

Consideriamo la variante del X problema di Hilbert in cui, dato un polinomio Q—come al solito a coefficienti interi—, si voglia stabilire se l'equazione $Q=0$ abbia o no soluzione sui *numeri naturali*, cioè sugli interi non-negativi. Si tratta di un problema piú facile, piú difficile, o di pari difficoltà del problema originario?

Torniamo a considerare un'istanza[4] $P=0$ del problema decisionale da cui siamo partiti. Evidenziamo le variabili distinte $V_1,\ldots,V_m$ che figurano in P scrivendo che $P \leftrightharpoons P(V_1,\ldots,V_m)$. Introduciamo nuove variabili $x_1,y_1,\ldots,x_m,y_m$, distinte una dall'altra, che spazino sui numeri naturali e poniamo $Q \leftrightharpoons P(x_1-y_1,\ldots,x_m-y_m)$; vale a dire: otteniamo il polinomio Q da P sostituendo, in P, ogni variabile V_i con la rispettiva espressione x_i-y_i. Ogni numero intero $\boldsymbol{v}$ può venir scritto come differenza $\boldsymbol{x}-\boldsymbol{y}$ di due numeri naturali; pertanto asserire che l'equazione $P=0$ è risolubile sugli interi equivale ad asserire che $Q=0$ è risolubile sui naturali. Se disponessimo di un algoritmo risolutore per la variante qui proposta del problema decisionale di Hilbert, potremmo dunque servircene per risolvere il problema originario: Dato P, lo trasformiamo in Q e poi verifichiamo se $Q=0$ sia risolubile o meno sui naturali.

Disponendo, viceversa, di un algoritmo risolutore per il problema decisionale originario, saremmo in grado di risolvere un'equazione polinomiale $Q=0$ nelle incognite *non-negative* $v_1,\ldots,v_m$? Occorre, a tal proposito, richiamare il *teorema dei quattro quadrati* (Lagrange, 1770): "Qualsiasi numero naturale può essere scomposto in somma di quattro quadrati perfetti". Ad esempio, $7=1+1+1+4=1^2+1^2+1^2+2^2$, $18=0+0+9+9=0^2+0^2+3^2+3^2$, o anche $18=0+1+1+16=0^2+(-1)^2+1^2+(-4)^2$. Potremmo dunque risolvere l'equazione $Q=0$ procedendo a questo modo: Trasformiamo $Q(v_1,\ldots,v_m)=0$ in $Q(W_1^2+X_1^2+Y_1^2+Z_1^2,\ldots,W_m^2+X_m^2+Y_m^2+Z_m^2)=0$ e verifichiamo se questa seconda equazione sia o no risolubile sugli interi.

Dunque i due problemi sono riducibili uno all'altro. In questo scritto riferiremo il 10º problema di Hilbert ad incognite naturali, senza alterarne la sostanza. Non cambierebbe granché se anche lo riferissimo a incognite intere *positive*:

Esercizio 6. *Mostrate che il 10º problema di Hilbert e la sua variante che riguarda incognite intere* positive *sono problemi riducibili uno all'altro.*

[4] Il termine tecnico *istanza* significa, a un bell'incirca: 'esemplare', 'caso particolare'.

Osservazione 7. *Adrien-Marie Legendre e a Carl Friedrich Gauss ottennero un raffinamento, noto come il* teorema dei tre quadrati*, del succitato teorema di Lagrange. Come osservato in [Mat71, pag. 253], tale teorema consente di triplicare—anziché quadruplicare—il numero delle incognite nella trasformazione di un'equazione diofantea sui naturali in equazione diofantea sugli interi. Il miglioramento della tecnica consiste nel trasformare l'equazione* $Q(v_1, \dots, v_m) = 0$ *nell'equazione* $Q(X_1^2 + X_1 + Y_1^2 + Z_1^2, \dots, X_m^2 + X_m + Y_m^2 + Z_m^2) = 0$.

Notazione 8. *In quanto segue, come abbiamo fatto in questo paragrafo, generalmente indicheremo le variabili di un polinomio con lettere latine maiuscole* $V, W, X, Y, Z, \dots$ *(talvolta munite di pedice) quando vorremo segnalare ch'esse spaziano sugli interi. Indicando le variabili con le minuscole* $v, w, x, y, z, \dots$*, segnaleremo invece che esse spaziano sui naturali. Le lettere in grassetto* $\boldsymbol{v}, \boldsymbol{x}, \boldsymbol{y}, \dots$ *denoteranno valori (per lo piú interi* $\geqslant 0$*) con cui sostituire omonime variabili.*

Le maiuscole P, Q, R, J, U *indicheranno polinomi. Le variabili di un polinomio, o espressioni che le rimpiazzano, saranno spesso evidenziate come illustrato dalle scritture* $P(x_1 - y_1, \dots, x_m - y_m)$ *ed* $R(\boldsymbol{a}_1, \dots, \boldsymbol{a}_n, z_1, \dots, z_\ell)$*. Quando, al contrario, vorremo disporre di una lettera entro cui* nascondere *la struttura interna di un polinomio, utilizzeremo il simbolo abbreviativo* $\leftrightharpoons$*, come su illustrato dalla scrittura* $Q \leftrightharpoons P(x_1 - y_1, \dots, x_m - y_m)$.

1.3 Problemi analoghi al X di Hilbert

Consideriamo la variante del X problema di Hilbert in cui, dato un polinomio P—come al solito a coefficienti interi—, si voglia stabilire se l'equazione $P = 0$ abbia o no soluzione sui *numeri reali*. Alfred Tarski scoprí nel 1930 un algoritmo per rispondere alle istanze di questo problema, ma circostanze storiche ritardarono fino al 1948 [Tar48] la pubblicazione del suo metodo.


Alfred Tarski (1902-1983)

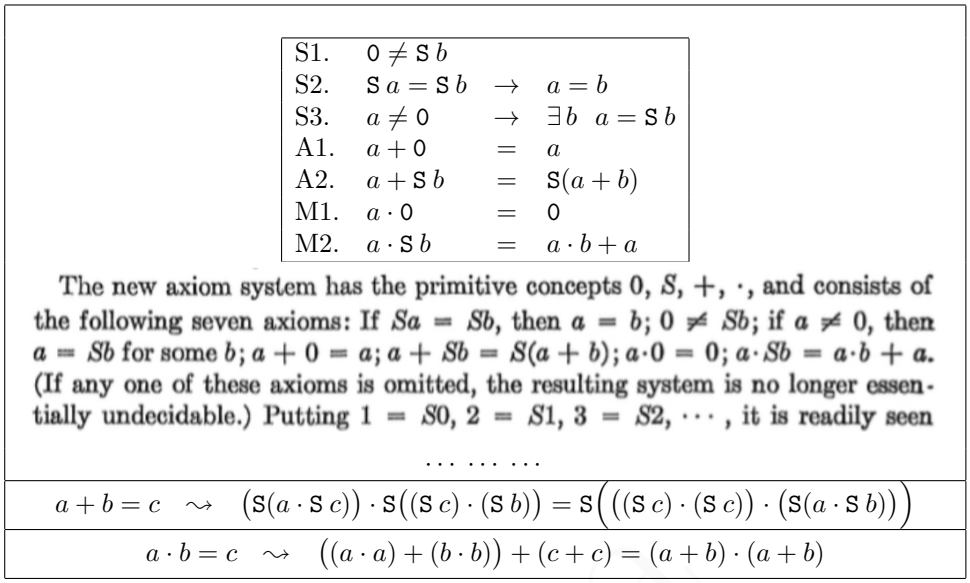
Varsavia–Berkeley

Consideriamo un'altra variante del X problema. Dato un polinomio P—sempre a coefficienti interi—, vogliamo stabilire se l'equazione $P = 0$ abbia o no soluzione sui *numeri razionali*. Ad oggi non sappiamo se esista un algoritmo per rispondere a questo problema.

In realtà, questo problema può essere visto come un sottoproblema del problema originariamente posto da Hilbert. Chiamiamo *omogeneo* un polinomio a coefficienti interi che sia somma di monomi tutti dello stesso grado. Raphael Mitchel Robinson dimostrò che

> Sono problemi tra loro equivalenti: (1) stabilire se un'arbitraria equazione diofantea abbia soluzione sui razionali; (2) stabilire se un'equazione diofantea omogenea abbia, sugli interi, soluzioni diverse da quella, banale, che assegna valore 0 a tutte le incognite. (Vedi [Mat93, pagg. 146–149]).


Raphael M. Robinson, 1911–1995



S1.	$0 \neq \mathtt{S}\, b$		
S2.	$\mathtt{S}\, a = \mathtt{S}\, b$	$\rightarrow$	$a = b$
S3.	$a \neq 0$	$\rightarrow$	$\exists b \;\; a = \mathtt{S}\, b$
A1.	$a + 0$	$=$	a
A2.	$a + \mathtt{S}\, b$	$=$	$\mathtt{S}(a + b)$
M1.	$a \cdot 0$	$=$	0
M2.	$a \cdot \mathtt{S}\, b$	$=$	$a \cdot b + a$

The new axiom system has the primitive concepts 0, S, $+$, $\cdot$, and consists of the following seven axioms: If $Sa = Sb$, then $a = b$; $0 \neq Sb$; if $a \neq 0$, then $a = Sb$ for some b; $a + 0 = a$; $a + Sb = S(a + b)$; $a \cdot 0 = 0$; $a \cdot Sb = a \cdot b + a$. (If any one of these axioms is omitted, the resulting system is no longer essentially undecidable.) Putting $1 = S0$, $2 = S1$, $3 = S2$, $\cdots$, it is readily seen

$\cdots \cdots \cdots$

$$a + b = c \quad \rightsquigarrow \quad \big(\mathtt{S}(a \cdot \mathtt{S}\, c)\big) \cdot \mathtt{S}\big((\mathtt{S}\, c) \cdot (\mathtt{S}\, b)\big) = \mathtt{S}\Big(\big((\mathtt{S}\, c) \cdot (\mathtt{S}\, c)\big) \cdot \big(\mathtt{S}(a \cdot \mathtt{S}\, b)\big)\Big)$$

$$a \cdot b = c \quad \rightsquigarrow \quad \big((a \cdot a) + (b \cdot b)\big) + (c + c) = (a + b) \cdot (a + b)$$

Figura 4: Sopra: Assiomi dell'aritmetica **Q** di R.M. Robinson [Rob52b].
Sotto: Eliminaz. del '+' proposta da J. Robinson [Rob49, pag. 100].
Sotto ancora: Riduzione del '$\cdot$' all'elevamento al quadrato.

1.4 L'*Entscheidungsproblem*

Che significa stabilire se un'equazione diofantea

$$P(\, z_1 \,, \ldots, \, z_m \,) \quad = \quad 0 \qquad (\dagger)$$

è risolubile, o meno, sui numeri naturali? Un modo d'intendere la questione è di riferirla a un sistema assiomatico che descriva—al meglio delle conoscenze che abbiamo su di essa—la struttura $(\, \mathbb{N} \,,\, 0 \,,\, 1 \,,\, + \,,\, \cdot \,)$ costituita dai naturali con somma, prodotto e rispettivi elementi neutri. Potremmo rifarci, quale *standard*, ai tardo-ottocenteschi *postulati di Peano*, noti anche come *assiomi dell'**aritmetica** di Dedekind-Peano*.[5]

In quest'ottica, la questione diventa:

[5] In assetto definitivo questi postulati si trovano nel lavoro di Giuseppe Peano *Formulaire de mathématiques*, t. II, § 2, Turin, Bocca Frères, 1898, p. VIII, pp. 1–15. In sostanza erano già presenti nella pubblicazione in latino di [Pea89], che ne indicava una fonte nello scritto *Was sind und was sollen die Zahlen?*, del 1888, del matematico tedesco Richard Dedekind. Una formulazione in termini odierni degli assiomi di Peano si trova in [Men97, pag. 155].

È possibile *dimostrare*, a partire dagli assiomi dell'aritmetica additivo-moltiplicativa dei naturali prescelta, l'enunciato

$$\exists\, z_1 \cdots \exists\, z_m \quad P_{\mathsf{sn}}(\, z_1\,, \ldots,\, z_m\,) \;=\; P_{\mathsf{dx}}(\, z_1\,, \ldots,\, z_m\,) \qquad (\ddagger)$$

che asserisce l'esistenza di valori $\boldsymbol{z}_i$ tali da soddisfare—se li mettiamo al posto delle rispettive variabili z_i—l'uguaglianza (†)?

Va da sé che, in (‡), il polinomio P è stato suddiviso in due polinomi a coefficienti non-negativi, secondo la convenzione introdotta con la Notazione 4.

Affinché quest'ottica deduttiva non svisi il X problema ci occorre un sistema assiomatico di una certa forza. Quale matematico si affannerebbe a cercare risposte alle istanze del X problema in un'aritmetica vistosamente debole come la teoria **Q** descritta in Fig. 4? Soffermiamoci, comunque, a esaminare questa teoria, per cogliere dove possano risiedere sue eventuali limitazioni; fra poco ne indicheremo ipotetiche estensioni $\mathbf{Q}^{+}$ e $\mathbf{Q}^{\#}$, ma senza darci pena di tentare una loro descrizione dettagliata.

Il linguaggio di **Q** comprende espressioni

$$\mathtt{0}\,,\quad \mathtt{S\,0}\,,\quad \mathtt{S\,S\,0}\,,\quad \mathtt{S\,S\,S\,0}\,,\quad \ldots$$

con cui possiamo designare, uno ad uno, i numeri $0, 1, 2, 3, \ldots$; dunque **Q** ci permette, grazie anche ai suoi costrutti $+$, $\cdot$ e $=$, di esprimere non solo i polinomi P_{sn} e P_{dx}, ma anche le affermazioni della forma

$$P_{\mathsf{sn}}(\, \underline{\boldsymbol{z}_1}\,, \ldots,\, \underline{\boldsymbol{z}_m}\,) \;=\; P_{\mathsf{dx}}(\, \underline{\boldsymbol{z}_1}\,, \ldots,\, \underline{\boldsymbol{z}_m}\,)\,,$$

dove stiamo impiegando $\underline{\boldsymbol{z}}$ per abbreviare l'applicazione reiterata del costrutto '*successivo di*' allo $\mathtt{0}$:

$$\underline{\boldsymbol{z}} \;=_{\text{Def}}\; \underbrace{\mathtt{S}\cdots\mathtt{S}}_{\boldsymbol{z}\text{ volte}}\,\mathtt{0}$$

(dunque ciascun $\underline{\boldsymbol{z}_i}$ designa il corrispondente numero $\boldsymbol{z}_i$). Un'aritmetica dovrebbe, se non altro, permetterci di determinare quale delle due opposte affermazioni

$$\begin{array}{rcl} P_{\mathsf{sn}}(\, \underline{\boldsymbol{z}_1}\,, \ldots,\, \underline{\boldsymbol{z}_m}\,) & = & P_{\mathsf{dx}}(\, \underline{\boldsymbol{z}_1}\,, \ldots,\, \underline{\boldsymbol{z}_m}\,)\,, \\ P_{\mathsf{sn}}(\, \underline{\boldsymbol{z}_1}\,, \ldots,\, \underline{\boldsymbol{z}_m}\,) & \neq & P_{\mathsf{dx}}(\, \underline{\boldsymbol{z}_1}\,, \ldots,\, \underline{\boldsymbol{z}_m}\,) \end{array}$$

sia quella vera, per ogni data m-upla $\langle \boldsymbol{z}_1, \ldots, \boldsymbol{z}_m \rangle$ di numeri naturali.

Fidiamoci di poter ottenere un'aritmetica $\mathbf{Q}^{+}$ che abbia tale potere dimostrativo, per *estensione* di **Q** (i.e. arricchendo, se occorre, la dotazione di assiomi di **Q**). Ecco allora come individuare—se c'è—una soluzione di (†):

Elencare sistematicamente le uguaglianze della forma

$$P_{\mathsf{sn}}(\, \underline{\boldsymbol{z}_1}\,, \ldots,\, \underline{\boldsymbol{z}_m}\,) \;=\; P_{\mathsf{dx}}(\, \underline{\boldsymbol{z}_1}\,, \ldots,\, \underline{\boldsymbol{z}_m}\,)\,,$$

senza alcuna tralasciarne e verificando ciascuna, fino a che una non risulti vera: a quel punto segnalare che (‡) è dimostrato.

Ma quando fermarci, se ci imbattiamo sempre in uguaglianze false? Questo non è un algoritmo decisionale, ma un procedimento algoritmico di *semi*-decisione!

Esercizio 9. *Escogitare in dettaglio come procedere, dato P, nell'elencazione di tutte le uguaglianze della forma $P_{\mathsf{sn}}(\underline{\boldsymbol{z}_1}, \ldots, \underline{\boldsymbol{z}_m}) = P_{\mathsf{dx}}(\underline{\boldsymbol{z}_1}, \ldots, \underline{\boldsymbol{z}_m})$.*

Un fatto importante della logica simbolica, fatto non difficile da appurare e tecnicamente non molto dissimile dall'Esercizio 9, è che

le dimostrazioni di un sistema assiomatico possono venir elencate

con un procedimento esaustivo. Pertanto, dovessimo accontentarci di un metodo di semi-decisione, ci si offrirebbe quest'altro candidato:

> Elencare una dopo l'altra tutte le dimostrazioni di $\mathbf{Q}^+$, fino a imbattersi in una la cui conclusione sia della forma
>
> $$P_{\mathsf{sn}}(\underline{\boldsymbol{z}_1}, \ldots, \underline{\boldsymbol{z}_m}) \quad = \quad P_{\mathsf{dx}}(\underline{\boldsymbol{z}_1}, \ldots, \underline{\boldsymbol{z}_m}),$$
>
> per opportuni numeri $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_m$: a quel punto segnalare che (‡) è del pari dimostrato.

È chiaro che se alla mera elencazione di tutte le possibili dimostrazioni potessimo sostituire un algoritmo $\mathfrak{A}$ in grado di dirci, data una qualsiasi congettura ϑ formulata nel linguaggio di $\mathbf{Q}^+$, se ϑ è dimostrabile *o no*, il procedimento sarebbe piú diretto e infinitamente piú utile: basterebbe somministrare ad $\mathfrak{A}$ la nostra tesi (‡) per vedercela accogliere o respingere. Hilbert venne maturando, negli anni, un progetto ben piú ambizioso di questo (in quanto non legato a una particolare aritmetica): risolvere l'*Entscheidungsproblem* (vedi Fig. 5).

L'algoritmo decisionale $\mathfrak{A}$ immaginato da Hilbert (vedi Fig. 6) riceverebbe come dati d'avvio due informazioni: **(1)** gli assiomi della teoria in esame, **(2)** la congettura ϑ; come risultato, dopo un lasso di tempo finito, $\mathfrak{A}$ fornirebbe una convalida di ϑ o un responso negativo. Come caso particolare, per risolvere il X problema, basterebbe somministrare ad $\mathfrak{A}$: (1) gli assiomi di $\mathbf{Q}^+$; (2) un enunciato della forma (‡).

Indipendentemente dall'*Entscheidungsproblem*, pensiamo a un'altra via per la risoluzione del X problema. Un'aritmetica davvero *completa* dovrebbe consentirci, per qualunque suo enunciato ϑ, di dimostrare o ϑ o la tesi contraria $\neg\,\vartheta$: delle due, infatti, una dev'essere vera. Nell'anno 1900, allorché Hilbert esponeva i suoi 23 problemi, non era escluso che l'aritmetica di Peano—ben piú forte di $\mathbf{Q}$, in quanto dotata del principio d'induzione—fosse completa.

In un'aritmetica completa, delle due opposte affermazioni

$$\begin{array}{lrcl} \exists\, z_1 \cdots \exists\, z_m & P_{\mathsf{sn}}(z_1, \ldots, z_m) & = & P_{\mathsf{dx}}(z_1, \ldots, z_m), \\ \forall\, z_1 \cdots \forall\, z_m & P_{\mathsf{sn}}(z_1, \ldots, z_m) & \neq & P_{\mathsf{dx}}(z_1, \ldots, z_m) \end{array} \qquad (\mathbf{II})$$

una (e una sola, a meno che gli assiomi non formino un sistema contraddittorio) sarà dimostrabile, per ogni P. Chi disponesse di un'aritmetica completa $\mathbf{Q}^{\#}$,

Entscheidungsproblem è il nome che Hilbert e Ackermann attribuiscono a quello che essi, nel 1928, giudicano il piú importante problema della logica. Descritto in termini approssimativi, il loro obiettivo è di escogitare un procedimento algoritmico che sappia stabilire ('decidere', secondo il frasario dei logici) se una proposizione matematica sia, o meno, conseguenza di un insieme finito di premesse assiomatiche.
Perché questa descrizione sia fedele alla concezione formalistica di chi proponeva il problema, occorre aggiungere che tanto la proposizione da vagliare che le premesse vanno espresse in un linguaggio simbolico di potere espressivo tale da consentire la formalizzazione dell'intero *corpus* delle discipline matematiche. Hilbert e Ackermann ravvisavano un adeguato *standard* formale nella logica predicativa del prim'ordine *piena*, ossia dotata di un'infinità numerabile di simboli di relazione a n posti per ogni intero $n > 0$.
Il primo impiego documentato del vocabolo *Entscheidungsproblem* da parte della scuola di Hilbert risale a una conferenza che Heinrich Behmann indirizzò, nel 1921, alla comunità matematica di Gottinga.

Figura 5: Il celebre 'problema della decisione' di Hilbert e Ackermann [HA28].

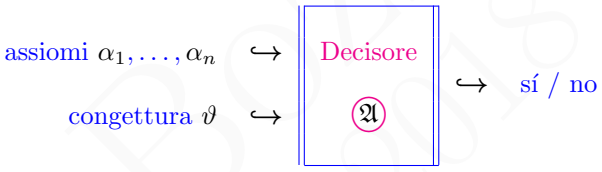


Figura 6: Schema di un ipotetico risolutore per l'*Entscheidungsproblem*. Il "sí" direbbe che una dimostrazione di ϑ esiste; il "no" che non esiste o addirittura che ϑ è *refutabile*, nel senso che dagli assiomi discende $\neg\vartheta$ anziché ϑ. Da assiomi deboli potrebbe anche non discendere né ϑ né $\neg\vartheta$ e anche in questo caso la risposta del decisore sarebbe "no".

potrebbe rispondere all'istanza del X problema di Hilbert riguardante il P dato procedendo a questo modo:

> Elencare una dopo l'altra tutte le dimostrazioni di $\mathbf{Q}^{\#}$ fino a raggiungimento di una delle due ipotesi contrapposte (**II**). Dare responso affermativo o negativo a seconda che sia stato dimostrato (‡) oppure il contrario.

Un metodo di *ricerca cieca* come questo sarebbe, a scopi pratici, inservibile—avrebbe tempi di risposta proibitivi—; a ogni modo, costituirebbe quanto richiesto dal X problema.

Gödel ha messo in chiaro nel 1931 [Göd31] che nessun'estensione non-contraddittoria dell'aritmetica di Peano può essere completa. In assenza di completezza, elencare le dimostrazioni in modo sistematico non garantisce un risultato: talvolta, nel caso di un'equazione insolubile, gli assiomi potrebbero non pronunciarsi né in un senso né nell'altro e la ricerca protrarsi per sempre.

1.5 Altra generalizzazione del X problema di Hilbert

Consideriamo ora equazioni della forma

$$E_{\mathsf{sn}} \quad = \quad E_{\mathsf{dx}}\,,$$

ove E_{sn} ed E_{dx} sono espressioni assemblate facendo uso dei seguenti costrutti:

- costanti intere non-negative (come ad es. 3, 0, 173),
- variabili che spaziano sui numeri naturali,
- gli operatori *diadici* (cioè, a due operandi) $\bullet + \bullet$, $\bullet \cdot \bullet$, $\bullet^{\bullet}$, di somma, prodotto, elevamento a potenza.

Consideriamo l'analogo del X problema di Hilbert riguardante equazioni di questo tipo — qui, ovviamente, ci chiediamo se l'equazione data sia risolubile sui naturali. Si tratta di un problema piú facile, piú difficile, o di pari difficoltà del problema originario?

Benché non stiamo piú utilizzando costanti negative, non abbiamo perso potere espressivo; difatti, come già notato, qualsiasi equazione diofantea *polinomiale* $P = 0$ può venir riscritta nella forma $P_{\mathsf{sn}} = P_{\mathsf{dx}}$, senza coefficienti negativi a sinistra né a destra. Viceversa, il linguaggio delle equazioni risulta piú ampio di prima, perché stiamo ammettendo variabili anche negli esponenti. Di primo acchito, possiamo dire di aver *esteso* il problema originario.[6]

In conversazioni con Raphael Robinson, verso la fine degli anni 1940, Alfred Tarski si dichiara convinto che non sia possibile esprimere l'operazione $b \mapsto 2^b$ (e dunque, men che meno, la $\langle a, b\rangle \mapsto a^b$) di esponenziazione tramite polinomi; ma come dimostrare quest'impossibilità?

Julia Robinson, 1919–1985

2 Due congetture temerarie

2.1 L'ipotesi di Julia Bowman Robinson

Julia Bowman Robinson [Csi08], che conseguirà nel 1948 il Ph.D. in matematica sotto la supervisione di Tarski, ha un'aspettativa opposta a quella di lui e

[6] Quando possono figurare ad esponente termini meno semplici delle costanti naturali, occorre cautela nell'impiego del '-'; altrimenti come, ad es., intendere il valore di $(x-y)^{2^{x-y}}$ per $x = 1$ ed $y = 3$? A scanso di ogni difficoltà con la sottrazione, in questo paragrafo abbiamo adottato il formato di equazione $E_{\mathsf{sn}} = E_{\mathsf{dx}}$ e messo al bando le costanti negative.

intuisce l'esistenza di un polinomio diofanteo $E(\,a\,,\,b\,,\,c\,,\,x_1\,,\ldots,\,x_m\,)$ tale che le terne $\langle \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\rangle$ di numeri naturali per cui l'equazione

$$E(\,\boldsymbol{a}\,,\,\boldsymbol{b}\,,\,\boldsymbol{c}\,,\,x_1\,,\ldots,\,x_m\,) \quad = \quad 0$$

ha soluzione in valori naturali delle incognite x_i siano precisamente quelle per cui è vero che $\boldsymbol{a}^{\boldsymbol{b}} = \boldsymbol{c}$.

Un tale E svolgerebbe un ruolo in certo qual modo analogo al sistema che nella Fig. 7 descrive le terne pitagoriche, ma con una differenza significativa: l'equazione $a^2 + b^2 - c^2 = 0$ è già di per sé polinomiale e pertanto le variabili aggiuntive che compaiono in figura—la x, la y e due variabili 'anonime'—servono solo a rendere l'elencazione delle terne pitagoriche piú diretta e agevole. Qui invece si tratta di specificare tramite polinomi una relazione che—almeno stando alla sua immediata caratterizzazione—parrebbe niente affatto 'diofantea'.

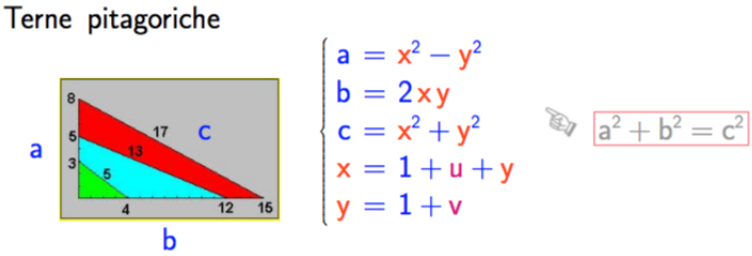


Figura 7: Polinomi per la generazione sistematica delle terne pitagoriche (i valori di a e b possono essere scambiati ed a, b, c possono venir moltiplicati per un comune fattore di scala).

L'ipotesi della Robinson poggia sul seguente 'indizio'. Com'era ben noto da tempo, le soluzioni dell'equazione[7]

$$x^2 - (\;\overbrace{\boldsymbol{a}^2 - 1}^{\boldsymbol{d}\;=_{Def}}\;)\,y^2 \quad = \quad 1\,, \quad \text{per} \quad \boldsymbol{a} = 2, 3, 4 \ldots\,,$$

sono gli assegnamenti

$$x \;\;\mapsto\;\; \boldsymbol{x_a}(\boldsymbol{b})\,, \qquad y \;\;\mapsto\;\; \boldsymbol{y_a}(\boldsymbol{b})\,, \qquad \text{con} \quad \boldsymbol{b} = 0, 1, 2 \ldots\,,$$

tali che

$$\boldsymbol{x_a}(\boldsymbol{b}) + \boldsymbol{y_a}(\boldsymbol{b})\,\sqrt{\boldsymbol{d}} \quad = \quad \left(\boldsymbol{a} + \sqrt{\boldsymbol{d}}\right)^{\boldsymbol{b}}\,;$$

questi numeri—peraltro irrazionali—crescono grosso modo come $\boldsymbol{a}^{\boldsymbol{b}}$ e dunque —intuitivamente parlando—c'è modo di descrivere una 'crescita esponenziale' tramite un'equazione diofantea.

[7] Quella che qui vediamo, è una forma particolare dell'equazione nota (a causa di uno sproposito di attribuzione dovuto a Eulero) come *equazione 'di Pell'*.

Che significa '*crescita esponenziale*'? E che senso ha voler descrivere una relazione a crescita esponenziale tramite un'equazione diofantea? Tali questioni vengono affrontate attorno al 1950 nell'articolo [Rob52a] di Julia Robinson. Alla prima la Robinson risponde:[8]

Definizione 1. *Si dice che un insieme* $\mathcal{J} \subseteq \mathbb{N}\times\mathbb{N}$ *è* A CRESCITA ESPONENZIALE *quando soddisfa le seguenti due condizioni:*

- $\mathcal{J}(\,a\,,\,b\,)$ *implica che* $b < a^a$*, per ogni* a *e ogni* b*;*
- *per ogni* k *in* $\mathbb{N}$*, ci sono numeri* a, b *per i quali* $\mathcal{J}(\,a\,,\,b\,)$ *ed* $a^k < b$*.*

(La prima condizione impedisce che b sia troppo grande rispetto ad a in una coppia di $\mathcal{J}$, mentre l'altra richiede che fra le b ve ne sia qualcuna non troppo piccola rispetto ad a; insieme, esse rivelano che b ha un andamento di crescita in certo senso esponenziale rispetto ad a).

Per esempio, l'insieme delle coppie $\langle \boldsymbol{a}, \boldsymbol{b}\rangle$ tali che $2^{\boldsymbol{a}} = \boldsymbol{b}$ soddisfa entrambe le condizioni.[9]

Ecco quanto Julia Robinson ipotizza riguardo alla seconda questione:

> **J.R.:** Esiste un polinomio diofanteo $J(\,a\,,\,b\,,\,y_1\,,\ldots,\,y_k\,)$ tale che le coppie di numeri naturali $\langle \boldsymbol{a}, \boldsymbol{b}\rangle$ per le quali l'equazione nelle incognite y_j
>
> $$J(\,\boldsymbol{a}\,,\,\boldsymbol{b}\,,\,y_1\,,\ldots,\,y_k\,) \;=\; 0$$
>
> ha soluzione su $\mathbb{N}$ formano un insieme $\mathcal{J}$ a crescita esponenziale.

Se ciò è vero, viene dimostrato nello stesso lavoro seminale [Rob52a], allora esiste un polinomio E soddisfacente i requisiti descritti all'inizio di questo paragrafo. Ma in tal caso la generalizzazione del X problema di Hilbert che abbiamo visto nel § 1.5 *non è* piú difficile del problema originario: a quello sarà, di fatto, riconducibile—una volta che sia dimostrata l'ipotesi J.R.—ogni istanza del problema generalizzato.

Annotazione di ordine psicologico. Come si spiega che apparisse controintuitiva, a Tarski, l'ipotesi J.R.? Forse perché vien naturale percepire una scala ascendente di potere espressivo nei costrutti

$$\mathtt{S}\,\bullet\,; \qquad \bullet + \bullet\,; \qquad \bullet \cdot \bullet\,, \qquad \bullet^2\,; \qquad 2^{\bullet}\,, \qquad \bullet^{\bullet}$$

d'incremento unitario, addizione, moltiplicazione ed elevamento al quadrato, e infine elevamenti a potenza; perciò è piú facile attendersi di poter esprimere un costrutto che in questa scala viene prima in termini di quelli che vengono dopo, che non il viceversa. La parte inferiore della Fig. 4 ci mostra: sopra,

[8] Di qui in poi designeremo, come è d'uso in letteratura:

$$\mathbb{N} =_{\text{Def}} \{0, 1, 2, \ldots\}, \qquad \mathbb{Z} =_{\text{Def}} \{0, \pm 1, \pm 2, \ldots\};$$

inoltre, $\mathbb{Q}$ ed $\mathbb{R}$ designeranno l'insieme dei numeri razionali e quello dei reali.

[9] Come è facile vedere, un numero finito di eccezioni—qui $\langle 0, 1\rangle$, $\langle 1, 2\rangle$, $\langle 2, 4\rangle$—è accettabile.

come esprimere l'addizione in termini di moltiplicazione e incremento unitario; sotto, come esprimere la moltiplicazione in termini di elevamento al quadrato e addizione. Queste possibilità di riscrittura non ci sconcertano; ma che si potesse ridurre l'elevamento a potenza ad addizione e moltiplicazione era, a dir poco, inatteso.

Esercizio 10. *Esprimere le operazioni* $\langle x, y\rangle \mapsto x+y$, $\langle x, y\rangle \mapsto x\cdot y$ *di addizione e moltiplicazione in termini dell'operazione* $\langle x, y\rangle \mapsto x^y$ *di elevamento a potenza.*

Anche la Robinson si aspetta che il X problema di Hilbert sia insolubile:

> "Per molte classiche equazioni diofantee con un parametro non è noto un metodo effettivo che, comunque venga fissato il parametro, dica se l'equazione ha soluzioni o no; perciò è poco plausibile che si possa trovare un procedimento di decisione. Ad esempio, non si conoscono metodi che determinino per quali valori di a il sistema diofanteo
>
> $$x^2 + a\,y^2 \;=\; s^2\,, \qquad x^2 - a\,y^2 \;=\; t^2$$
>
> è risolubile. (Primi a studiare questo problema furono gli Arabi, nel Medio Evo)." [Rob52a, pagg. 437–438]

2.2 L'ipotesi di Martin Davis

Martin D. Davis, 1928–

Nella tesi di dottorato di M. Davis, approvata dalla Princeton University nel maggio 1950 [Dav50], compare una congettura temeraria: che le relazioni n-adiche

$$\mathcal{R} \;\subseteq\; \mathbb{N}^n$$

sui naturali le cui n-uple sono elencabili in maniera effettiva (cioè tramite un procedimento algoritmico) siano tutte e sole le relazioni che possono venir caratterizzate per mezzo di un polinomio diofanteo R a questa maniera:

$$\begin{array}{c}\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\rangle \in \mathcal{R} \text{ se e solo se ha soluzione su } \mathbb{N} \text{ l'equazione} \\ R(\,\boldsymbol{a}_1\,, \ldots,\, \boldsymbol{a}_n\,,\, x_1\,, \ldots,\, x_m\,) \;=\; 0\,;\end{array} \qquad (\oplus)$$

In effetti egli si accostava molto a questo traguardo, riuscendo a individuare un polinomio diofanteo Q tale che

> $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\rangle \in \mathcal{R}$ se e solo se, per qualche $\boldsymbol{z}$ in $\mathbb{N}$, ha soluzione su $\mathbb{N}$ ciascuna delle equazioni
>
> $$\begin{array}{rcl} Q(\,\boldsymbol{a}_1\,, \ldots,\, \boldsymbol{a}_n\,,\, v_1\,, \ldots,\, v_\ell\,,\, \boldsymbol{0}\,,\, \boldsymbol{z}\,) & = & 0\,, \\ Q(\,\boldsymbol{a}_1\,, \ldots,\, \boldsymbol{a}_n\,,\, v_1\,, \ldots,\, v_\ell\,,\, \boldsymbol{1}\,,\, \boldsymbol{z}\,) & = & 0\,, \\ \vdots & \vdots & \vdots \\ Q(\,\boldsymbol{a}_1\,, \ldots,\, \boldsymbol{a}_n\,,\, v_1\,, \ldots,\, v_\ell\,,\, \boldsymbol{z}\,,\, \boldsymbol{z}\,) & = & 0\,. \end{array}$$

All'epoca le relazioni 'elencabili in maniera effettiva' erano già ben studiate in teoria della computabilità, dove si chiamano PREDICATI ENUMERABILI RICORSIVAMENTE. Era noto, tra l'altro, ch'esse formano una classe chiusa rispetto alle operazioni d'intersezione e di unione (quando il numero di argomenti dei predicati-operandi è lo stesso), ma *non* rispetto alla complementazione—può accadere, cioè, che una $\mathcal{R}$ inclusa in $\mathbb{N}^n$ sia ricorsivamente enumerabile mentre $\mathbb{N}^n \setminus \mathcal{R}$ non lo è.

I predicati DIOFANTEI, cioè rappresentabili nella forma ($\oplus$) erano, invece, un classe di relazioni relativamente poco conosciuta.

La '*rappresentazione normale*' di Davis di un $\mathcal{R}$ enumerabile ricorsivamente viene di solito scritta, in breve:

$$\begin{aligned} \langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \rangle \in \mathcal{R} \quad \leftrightarrow \quad & \exists\, z\ (\forall\, y \leqslant z)\ \exists\, v_1 \cdots \exists\, v_\ell \\ & Q(\,\boldsymbol{a}_1\,, \ldots,\, \boldsymbol{a}_n\,,\, v_1\,, \ldots,\, v_\ell\,,\, y\,,\, z\,) \quad = \quad 0\,. \end{aligned} \tag{$\otimes$}$$

Qui il costrutto $\forall\, y \leqslant z$, da leggersi "per ogni y, fino a z compreso, si ha che…", designa la *quantificazione universale limitata*. Davis si domandava: possiamo riformulare ($\otimes$) in modo da sbarazzarci di questo costrutto, che intriga? Riteneva di sí e si rendeva conto che riuscire in quest'intento avrebbe comprovato l'insolubilità algoritmica del X problema (vedi Fig. 8).

If we could also prove that the class of diophantine predicates is closed under bounded universal quantification, then it would follow from 2.7 that every recursively enumerable predicate is diophantine.

But this clearly would lead to the unsolvability of the general decision problem for diophantine equations in non-negative integers, and hence--by the remarks of §1--of Hilbert's tenth problem.

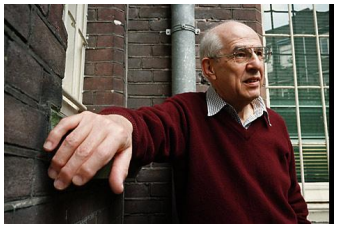
Now, evidently every diophantine predicate is recursively enumerable. If we also knew the converse of this result, then we should of course be able to answer the above question in the affirmative, with all the attendant consequences. Hence our investigation of the relation between diophantine predicates and recursively enumerable predicates.

Figura 8: La 'daring hypothesis' di Davis [Dav50, pag. 84 e pag. 80].

Senza peraltro esibirne in concreto nessuno, Davis dimostrava che esistono predicati diofantei il cui complementare non è diofanteo. Ciò è solo un indizio, ma corrobora l'ipotesi che i predicati diofantei e quelli enumerabili ricorsivamente formino la stessa classe.

Esercizio 11. *Date evidenza del fatto che ogni predicato diofanteo è enumerabile ricorsivamente.*

Osservazione 12. *Nel 1956, con una costruzione molto diversa da quella di Davis, Raphael Robinson riuscirà a fissare $\ell = 4$ nella rappresentazione normale ($\otimes$), rendendo cosí ℓ indipendente da $\mathcal{R}$; Robinson stesso ridurrà questo valore a $\ell = 3$ nel 1972; sempre nel 1972, Yuri Matiyasevich lo abbasserà ad $\ell = 2$.*



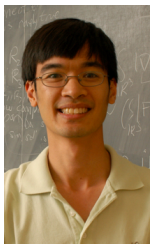
Hilary Putnam,
1926–2016

2.3 Il teorema Davis-Putnam-Robinson

> "It was in the summer of 1959 that Hilary and I really hit the jackpot. We decided to see how far we could get with the approach we had used at the Logic Institute in Ithaca, if, following Julia Robinson's lead, we were willing to permit variable exponents in our Diophantine equations." [Dav99, pag. 68]

Nel 1959 Martin Davis e Hilary Putnam scrivono il rapporto di ricerca [DP59] e ne sottomettono la parte finale per la pubblicazione come articolo scientifico, ma poco dopo la ritirano. Il lavoro sottomesso e ritirato dimostra che

> se, *per ogni n, ci sono n numeri primi in progressione aritmetica*, allora ogni predicato enumerabile ricorsivamente può venir definito esistenzialmente in termini di polinomi e della funzione $y = 2^x$.



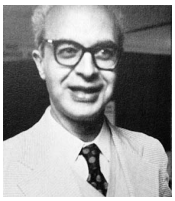
Terence Tao,
1975–
Fields medal 2006

All'epoca gli autori chiamano *ipotesi P.A.P.* la premessa (qui in corsivo) che condiziona quest'affermazione; tale 'ipotesi di lavoro' diverrà un teorema solo nel 2004, grazie a Ben Green e a Terence Tao [TG08]. Cosí oggi noi possiamo considerare il risultato di Davis e Putnam una dimostrazione completa del fatto che ogni predicato enumerabile ricorsivamente è esistenzialmente definibile in termini di 'polinomi esponenziali' diofantei. Ad accelerare il corso degli eventi, come Martin Davis narra nella propria autobiografia [Dav99], è l'apporto di Julia Robinson: lei semplifica la dimostrazione originaria di Davis e Putnam e riesce a fare a meno dell'ipotesi P.A.P.: nel 1961, i tre pubblicano assieme il celebre teorema Davis-Putnam-Robinson [DPR61].

Nel recensire l'articolo [DPR61], Georg Kreisel prende un celebre abbaglio:

> "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.



(Georg Kreisel, 1923–2015)

> 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]

Per meglio mettere in luce la portata del teorema Davis-Putnam-Robinson nello studio del 10° problema di Hilbert, indichiamo con $\mathfrak{D}$, $\mathfrak{E}$, $\mathfrak{R}$ le collezioni di predicati che il rapporto [DP59] di Davis e Putnam chiamava: *diofantei*, *definibili esistenzialmente* ed *enumerabili ricorsivamente* ('*r.e.*' in inglese).[10] Le inclusioni $\mathfrak{D} \subseteq \mathfrak{E} \subseteq \mathfrak{R}$ sono facili da verificare; tutt'altro che ovvio, invece, è ch'esse valgano come uguaglianze. Le 'ipotesi'—o, per dir meglio, congetture (vedi sopra, § 2.1 e § 2.2)—che Julia Robinson e Martin Davis avevano avanzato attorno al 1950 asserivano, rispettivamente, che

- esistono predicati Diofantei ad andamento esponenziale di crescita—onde $\mathfrak{D} = \mathfrak{E}$;
- $\mathfrak{D} = \mathfrak{R}$.

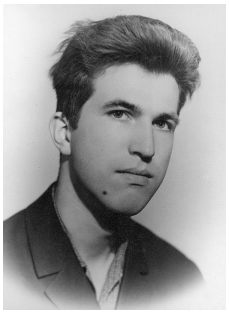
Davis e Putnam partivano dalla forma normale ($\otimes$) di Davis e mostravano come l'espressività in piú derivante dalla libertà di utilizzare esponenti variabili e dalla loro assunzione P.A.P. consentisse di dimostrare il teorema Davis-Putnam-Robinson, ossia che $\mathfrak{E} = \mathfrak{R}$. Cosí l'ipotesi di Davis—e, conseguentemente, la risposta al 10° problema di Hilbert—venivano ricondotte all'ipotesi J.R., che sarà dimostrata nel 1970.

Esercizio 13. *Perché l'uguaglianza* $\mathfrak{E} = \mathfrak{R}$ *implica l'insolubilità algoritmica del X problema? (Suggerim.: Si dimostri che ogni predicato decidibile è enumerabile ricorsivamente e si sfrutti il fatto, poco fa dato per noto, che* $\mathfrak{R}$ non è *chiuso rispetto alla complementazione).*

3 Risoluzione negativa del X problema

3.1 Il teorema di Matiyasevich (1970)

Chi apporta il contributo decisivo alla 'soluzione negativa' del X problema è Yuri Vladimirovich Matiyasevich, che all'età di 22 anni riesce a specificare mediante polinomi diofantei una relazione a crescita esponenziale.



Yuri V. Matiyasevich, 1947–

[10] La definizione di predicato diofanteo è stata già richiamata nel § 2.2; quella di predicato definibile esistenzialmente è ad essa analoga, ma impiega 'polinomi esponenziali' (in cui può figurare il costrutto di esponenziazione) al posto dei polinomi. La nozione di predicato enumerabile ricorsivamente è stata sbozzata nel § 2.2, ma abbisogna di ulteriori chiarimenti.

> "Prior to this paper, the existence of such a Diophantine relation was widely disbelieved. Thus, its discovery is a crucial step in our understanding of Diophantine equations." (J. Robinson, [Rob72])

Dalla scoperta del russo consegue che, cosí come avevano anticipato Post e Davis,

il decimo problema di Hilbert *non è* algoritmicamente risolubile.

La relazione in questione è l'insieme delle coppie $\langle \boldsymbol{u}\,,\ \boldsymbol{v}\rangle$, in cui $\boldsymbol{v}$ è il $2\boldsymbol{u}$-esimo numero della progressione costituita dai *numeri di Fibonacci*

$$\mathrm{F}_0 \;=\; 0\,, \qquad \mathrm{F}_1 \;=\; 1\,, \qquad \mathrm{F}_{n+1} \;=\; \mathrm{F}_n + \mathrm{F}_{n-1}\,.$$

La crescita esponenziale (che ha lo stesso andamento di $\big((1+\sqrt{5})/2+1\big)^n$, cfr. [Mat92]) si dimostra attraverso le disequazioni, soddisfatte per $n = 1, 2, 3, \ldots$:

$$n \;\leqslant\; 2^{n-1} \;\leqslant\; \mathrm{F}_{2\,n} \;<\; 3^n\,.$$

Storicamente, la prima specifica diofantea della relazione

$$\{\, \langle \boldsymbol{u}\,,\, \mathrm{F}_{2\,\boldsymbol{u}}\rangle \;:\; \boldsymbol{u} \in \mathbb{N} \setminus \{0\}\,\}$$

è quella mostrata in Fig. 9: essa comparirà, lievemente snellita, in [Mat70a]).[11] Martin Davis la riecheggerà pochi mesi dopo [Dav71], utilizzando in maniera personale i metodi nuovamente sviluppati da Matiyasevich per ottenere un sistema alternativo di equazioni—quello che mostriamo in Fig. 10, poi perfezionato in [Dav73])—che porta (e in maniera piú diretta) al medesimo risultato.

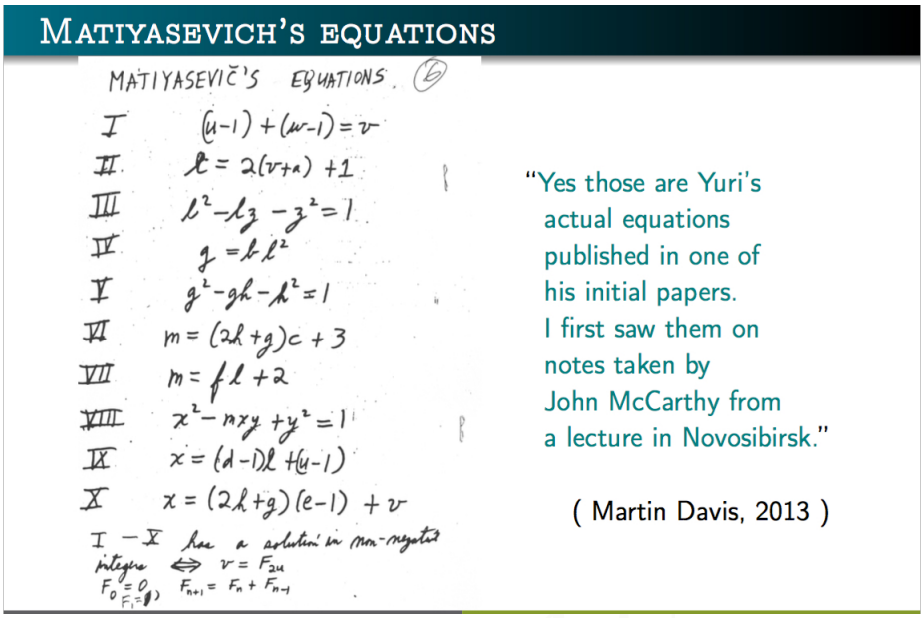
Osservazione 14. *Già nel 1966 (come egli riporta in [Mat92]) Matiyasevich aveva scoperto che affinché f sia un F_n basta e occorre che vi sia un intero $x > 0$ per cui vale $f^2 - f\,x - x^2 = \pm 1$; ciò implicava, ovviamente, la diofanticità dell'*insieme *dei numeri di Fibonacci ma non dimostrava l'ipotesi J.R..*

3.2 Sentieri interrotti

È immaginabile che l'insolubilità algoritmica del X problema potesse rivelarsi per vie diverse dalla dimostrazione dell'ipotesi J.R. ottenuta da Matiyasevich?

Alla vigilia del risultato conclusivo di lui, la stessa Julia Robinson prospettava in [Rob69] una via alternativa: individuare un predicato 1-adico (cioè una proprietà) diofanteo, che sia soddisfatto da un'infinità di numeri e solo da numeri primi. Oggi sappiamo che la *primalità* stessa, cioè la proprietà soddisfatta

[11] L'"ago nel pagliaio' la cui individuazione permise a Matiyasevich di ottenere il suo importante risultato è l'implicazione: $\boxed{\text{se } \mathrm{F}_n^2 \text{ divide } \mathrm{F}_m \text{ allora } \mathrm{F}_n \text{ divide } m}$. Per dimostrare questa, Matiyasevich sfruttò un teorema ottenuto sin dal 1942 dal matematico sovietico Nikolai N. Vorob'ev, registrato solo nella terza edizione di un celebre trattato di costui sui numeri di Fibonacci, apparsa nel 1969. Ebbe un influsso determinante, nella scoperta di Matiyasevich, la lettura di un articolo di Julia Robinson di quello stesso anno: [Rob69]. (Vedi [Csi08]).



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

Leonardo Pisano
Fibonacci,
ca. 1170 – ca. 1250

Figura 9: Riportiamo qui un sistema di equazioni tratto da [DH73], che mostriamo anche 'condensato' in una singola equazione polinomiale. Nel 1970, tramite questo sistema, il matematico russo Yuri Vladimirovich Matiyasevich forní una soluzione negativa al decimo problema di Hilbert. I valori delle variabili u e v nelle soluzioni, su $\mathbb{N}\setminus\{0\}$, del sistema sono tutte e sole le coppie $\langle \boldsymbol{u},\, \boldsymbol{v}\rangle$ per le quali $\boldsymbol{v}$ è il $2\,\boldsymbol{u}$-esimo numero di Fibonacci.

da tutti e soli i numeri primi, è un predicato di tal natura. Questo fatto consegue dal teorema di Matiyasevich—vedi sotto, § 3.4—; forse, però, la scoperta avrebbe potuto svilupparsi in senso inverso.

Anche Davis aveva, all'antivigilia del risultato di Matiyasevich, prospettato un'altra via: per far emergere l'insolubilità del X problema, osservava Davis,

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

Figura 10: In tutte queste equazioni le variabili spaziano su $\mathbb{N}$. (Per aderenza a [Dav71], sfruttiamo anche lettere greche—α, β, γ, δ, ζ, η, ξ—per denotare qualche variabile). Le equazioni (I)–(X) nei parametri u, v, a hanno soluzione per $a > 1$ se e solo se $v = \boldsymbol{y}_u(a)$, dove $X = \boldsymbol{x}_u(a)$, $Y = \boldsymbol{y}_u(a)$ è la $u+1$–esima soluzione, su $\mathbb{N}$, dell'equazione di Pell $X^2 - (a^2-1)\,Y^2 = 1$. Le equazioni (I)–(XV) nei parametri α, β, u hanno soluzione per $\beta \geqslant 1$ se e solo se $\alpha = \beta^u$.

sarebbe bastato dimostrare che l'equazione

$$9\,(x^2 + 7\,y^2)^2 - 7\,(u^2 + 7\,v^2)^2 \;=\; 2$$

ha *una sola* soluzione (vedi sopra, Esercizio 5). Gregory V. Chudnovsky, un russo di qualche anno piú giovane di Matiyasevich, sostenne di essere giunto per via indipendente a una dimostrazione dell'ipotesi J.R. utilizzando l'equazione di Davis (vedi [Dav10, pag. 156]); di questa scoperta gli dà credito, a quanto pare, anche [Man77, pag. 206]. Però qualcosa non quadra, in quanto la 'quaternaria quartica' di Davis *non ha* una sola soluzione come egli si aspettava. Una seconda venne scoperta fra il 1971 e il 1972, numerose altre vengono presentate in [SW95]. Quest'ultimo articolo, del 1995, punta ad avvalorare l'ipotesi che l'equazione di Davis abbia *infinite* soluzioni; lo fa sulla scorta di poche decine di soluzioni, cosicché l'ipotesi resta opinabile: su ciò, difatti, vediamo oggi contrapporsi due congetture. Il dibattito mantiene una certa attualità in quanto, come osservato da Julia Robinson, l'insolubilità del X problema di Hilbert avrebbe

Andrej A. Markov Jr., 1903–1979

potuto discendere dalla verifica che l'equazione di Davis ha in tutto *un numero finito* di soluzioni.

Il matematico sovietico Andrej Andreevich Markov Jr., avendo notato che ogni equazione fra parole su un alfabeto di due simboli poteva essere tradotta in un sistema di equazioni diofantee, si aspettava che una dimostrazione d'insolubilità del X problema di Hilbert sarebbe stata ottenuta mostrando l'insolubilità algoritmica del problema decisionale della parola per semigruppi liberi. Molti, inclusi—negli anni 1970—gli stessi Yu. Matiyasevich, M. Davis, J. Robinson, lavorarono in questa direzione fin quando un (intricato!) algoritmo decisionale che risolveva il problema posto da Markov non venne scoperto, nel 1977, da Gennadij Semenovich Makanin [Mak77].

3.3 Risvolti positivi di una soluzione negativa

(Il titolo di questo paragrafo fa eco a quello del celebre [DMR76], articolo del quale qui e nel § 3.4 vengono riprese in chiave minore alcune considerazioni).

I teoremi di Davis-Putnam-Robinson e di Matiyasevich implicano che, per ogni

$$f: \quad \mathbb{N}^n \quad \rightharpoonup \quad \mathbb{N}$$

funzione computabile parziale, si può trovare un polinomio P a coefficienti interi tale che per ogni $n+1$-upla $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n, \boldsymbol{\kappa} \rangle$ valga la bi-implicazione

$$f(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) = \boldsymbol{\kappa} \quad \leftrightarrow \quad \exists x_0 \cdots \exists x_m \quad P(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n, x_0, x_1, \ldots, x_m) = \boldsymbol{\kappa}$$

(dove tutte le variabili rappresentano numeri interi non-negativi).

Spiegazione. f è PARZIALE (come abbiamo inteso segnalare impiegando $\rightharpoonup$ al posto di $\longrightarrow$) nel senso che possono esservi n-uple $\vec{\boldsymbol{a}} = \langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \rangle$ cui la f non associa alcuna immagine — in termini informatici, ciò potrebbe significare che l'esecuzione del programma che computa f non termina quando gli viene somministrato $\vec{\boldsymbol{a}}$. Come casi-limite, le n-uple prive d'immagine potrebbero formare l'intero $\mathbb{N}^n$ oppure l'insieme vuoto.

In quelle $\vec{\boldsymbol{a}}$ per cui $f(\vec{\boldsymbol{a}})$ rimane indefinito, risulta $P(\vec{\boldsymbol{a}}, \vec{\boldsymbol{x}}) < 0$ per qualsiasi $\vec{\boldsymbol{x}} \in \mathbb{N}^{m+1}$. Quelle $\vec{\boldsymbol{a}}$ cui $f(\vec{\boldsymbol{a}})$ associa un'immagine avranno $P(\vec{\boldsymbol{a}}, \vec{\boldsymbol{x}}) \geqslant 0$ in almeno un caso; e, in corrispondenza a tali n-uple, il valore non-negativo $\boldsymbol{\kappa}$ assunto da P sarà sempre lo stesso. ⊣

Questa caratterizzazione delle funzioni computabili istituisce un formidabile ponte fra la teoria della computabilità e la teoria dei numeri.

Ad esempio, la congettura di Christian Goldbach (ca. 1742), "ogni numero pari maggiore di 2 può essere scritto come somma di due primi" non ha, *prima facie*, l'aspetto di un'istanza del X problema.[12] Purtuttavia:

[12] Hilbert, in effetti, menziona la congettura di Goldbach sotto l'*ottavo* dei suoi 23 problemi.

Esempio 15. *Consideriamo la funzione*

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

definita su tutto $\mathbb{N}$*, a valori 0/1. Poiché questa* g *è computabile, possiamo individuare un polinomio diofanteo* $G(\,a\,,\,x_0\,,\ldots,\,x_m\,)$ *tale che*

$$g(\,\boldsymbol{a}\,) = \boldsymbol{\kappa} \quad \leftrightarrow \quad \exists\, x_0 \cdots \exists\, x_m \quad G(\,x_0\,, x_1\,, \ldots,\, x_m\,,\,\boldsymbol{a}\,) = \boldsymbol{\kappa}\,.$$

E ora domandiamoci: è risolubile l'equazione

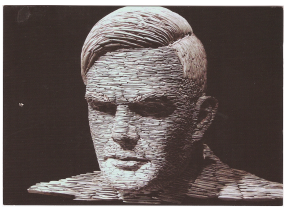
$$G(\,x_0\,, x_1\,, \ldots,\, x_m\,, x_{m+1}\,) = 0 \;\; ?$$

La risposta, evidentemente, è affermativa o negativa a seconda che sia falsa o vera la congettura in esame. Abbiamo dunque riscritto la congettura come istanza del X problema.

Perennemente inquieta, la ricerca oggi si domanda:

- Potremmo, nel costruire P a partire da una specifica formale di f, far sí che sia una sola la $\vec{\boldsymbol{x}}$ per cui vale $P(\vec{\boldsymbol{a}}, \vec{\boldsymbol{x}}) = f(\vec{\boldsymbol{a}})$—se questo valore esiste, beninteso? O, quanto meno, garantire che l'insieme di tali $m+1$-uple sia finito? (Nel caso-chiave $\langle a, b\rangle \overset{f}{\mapsto} a^b$, nessuno ancora c'è riuscito).
- Ammettiamo d'imporre, in base alla taglia delle $\boldsymbol{a}_1\,,\ldots,\,\boldsymbol{a}_n$ date, una limitazione di taglia alle componenti $\boldsymbol{x}_0\,,\,\boldsymbol{x}_1\,,\ldots,\,\boldsymbol{x}_m$ di una $\vec{\boldsymbol{x}}$ risolutiva. Con ciò ascriveremo f a una particolare classe di complessità algoritmica. Possiamo, per questa via, formulare gerarchie di complessità che gettino luce su problematiche tuttora irrisolte nello studio della computabilità?

Passiamo ora a considerare la questione dell'UNIVERSALITÀ, nozione fondante dell'informatica a partire dallo studio di Alan Mathison Turing del 1936:



Alan M. Turing
1912–1954

> " It is possible to invent a single machine which can be used to compute any computable sequence. If this machine I is supplied with a tape on the beginning of which is written the $S.D$ of some computing machine M, then I will compute the same sequence as M. In this section I explain in outline the behavior of the machine. The next section is devoted to giving the complete table for I. " [Tur36]

La seconda parte della citazione riportata a pag. 17 alludeva a una conseguenza *affatto implausibile*—a giudizio di Kreisel—dell'ipotesi di Davis. Implausibile ma (col senno di poi) vera, giacché discende dal teorema di Matiyasevich:

Equazioni diofantee universali. Per ogni $n \in \mathbb{N}$, esiste un'equazione diofantea polinomiale

$$U(a_1, \ldots, a_n, a_{n+1}, x_1, \ldots, x_m) \quad = \quad 0$$

tale che i predicati diofantei n-adici sono tutti e soli i predicati definiti da una delle equazioni

$$U(a_1, \ldots, a_n, \boldsymbol{k}, x_1, \ldots, x_m) \quad = \quad 0$$

che risultano dal variare di $\boldsymbol{k}$ in $\mathbb{N}$.

(L'ultimo parametro, a_{n+1} , è impostabile, $\boldsymbol{k}$ ne è l'impostazione)

A un lettore accorto, già il teorema Davis-Putnam-Robinson poteva rivelare un risultato dello stesso genere ma assai meno pregnante:

Per ogni $n \in \mathbb{N}$, esiste un polinomio esponenziale

$$U_{\mathsf{xp}}(a_1, \ldots, a_n, a_{n+1}, x_1, \ldots, x_m)$$

tale che i predicati n-adici definibili esistenzialmente sono tutti e soli i predicati definiti da una delle equazioni

$$U_{\mathsf{xp}}(a_1, \ldots, a_n, \boldsymbol{k}, x_1, \ldots, x_m) \quad = \quad 0$$

che risultano dal variare di $\boldsymbol{k}$ in $\mathbb{N}$.

Ciò non veniva detto a chiare lettere, ma pressappoco in questa forma:

Esiste un polinomio diofanteo

$$U(a, k, x_1, \ldots, x_m, y_1, \ldots, y_m)$$

tale che i predicati 1-adici definibili esistenzialmente sono tutti e soli i predicati definiti da una delle equazioni

$$U(a, \boldsymbol{k}, x_1, \ldots, x_m, 2^{x_1}, \ldots, 2^{x_m}) \quad = \quad 0$$

che risultano dal variare di $\boldsymbol{k}$ in $\mathbb{N}$.

Esercizio 16. *Nell'enunciato del teorema sulle* equazioni diofantee universali *si potrebbe sostituire la locuzione 'predicati diofantei' con la 'predicati enumerabili ricorsivamente'? Negli enunciati dei due teoremi che lo seguono, si sarebbe potuto (già prima della scoperta di Matiyasevich) sostituire 'predicati definibili esistenzialmente' con 'predicati enumerabili ricorsivamente'?*

A che poteva riferirsi, Kreisel, nel suo incauto giudizio d'implausibilità, con le parole "uniformly reducible to those in a fixed number of variables $\cdots$"? Per tentare una risposta, indichiamo con $\mathrm{U}(a\,,k\,,x_1,\ldots,x_{m_\star})$ il polinomio universale associato ai predicati diofantei 1-adici. Lasciamo al lettore la verifica che, per ogni n in $\mathbb{N}$, un accettabile pol. universale per i predicati diofantei n-adici è lo

$$U_n(\,a_1\,,\ldots,\,a_n\,,\,k,\,x_1\,,\ldots,\,x_{m_\star}\,) \quad =_{\mathrm{Def}} \quad \mathrm{U}\big(\,\kappa_n(\,a_1\,,\ldots,\,a_n\,)\,,\,k\,,\,x_1\,,\ldots,\,x_{m_\star}\big)\,,$$

dove ciascun κ_n designa un polinomio in n variabili e a coefficienti in $\mathbb{N}$, *iniettivo* in quanto funzione da $\mathbb{N}^n$ in $\mathbb{N}$.

Come stiamo vedendo, il numero $m_\star$ delle incognite resta sempre lo stesso. Detiene il *record* di minimo val. noto di $m_\star$, dal 1977 a oggi, il numero 9 [Jon82].

Esercizio 17. *Dimostrare, per $n = 0, 1, 2, \ldots$, l'iniettività del polinomio*

$$\kappa_n(\,y_1\,,\ldots,\,y_n\,) \quad =_{Def} \quad \sum_{i=1}^{n}\Big(\sum_{j=1}^{i} y_j\Big)^i$$

di Nikolaj Kirillovič Kosovskiĭ [Kos71].

Osservazione 18. *La costruzione di un polinomio diofanteo universale fu favorita, al tempo della sua scoperta, da un armamentario concettuale di stampo novecentesco. Matiyasevich non può far a meno di osservare che*

> "In contrast with number theory, computability theory had dealt for a long time with objects analogous to universal equations, in particular, with creative sets, universal Turing machines, normal forms for partial recursive functions, and so on." *[Mat93, pag. 69]*

Tuttavia egli poi rileva—con una certa soddisfazione, direi—che il lavoro [MR75] scritto assieme alla Robinson ha migliorato i risultati sulle equazioni diofantee "by using new number-theoretic results instead of the results from computability theory that had originally been used".

Sempre nel contesto di [Mat93, pag. 69], il matematico russo conclude che "Ultimately these techniques led to the purely number-teoretic construction introduced in this chapter".

3.4 Polinomi che rappresentano o generano i primi

> "The search for "explicit formulas" for prime numbers was a traditional occupation of dedicated number theory enthusiasts for many centuries. Euler found the polynomial $x^2 + x + 41$, which takes a long series of only prime values. But it has long been known that the set of values at integer points of a polynomial f in $\mathbb{Z}[x_1, \ldots, x_n]$ cannot consist entirely of prime numbers $[\cdots]$" [Man77, pp. 207/208]

In che modo un polinomio può rappresentare i numeri primi? In [Rob52a, pagg. 446–447], la Robinson osservava che sono definibili esistenzialmente (cioè

appartengono ad $\mathfrak{E}$, vedi § 2.3) le relazioni (una a 3 argomenti, l'altra a 2)

$$\left(\begin{array}{c} a \\ b \end{array} \right) \quad = \quad c\,, \qquad a\,! \quad = \quad c\,,$$

dove $\binom{a}{b}$ ed $a!$ designano il *coefficiente binomiale* e la funzione *fattoriale*.[13] Di conseguenza è definibile esistenzialmente la proprietà

$$\exists\, k\, \exists\, u\, \exists\, v\, \big(\quad p \quad = \quad 2 + k \quad \& \quad p\, u - (k+1)!\, v \quad = \quad 1 \quad \big)\,,$$

soddisfatta da tutti e soli quei numeri $p \geqslant 2$ che non hanno divisori, tranne l'1, in comune[14] con il rispettivo fattoriale $(p-1)\,!$. Tali p sono, evidentemente, i *numeri primi*. Pertanto, non appena l'ipotesi J.R. fosse risultata vera, si sarebbe potuto individuare un pol. diofanteo $P(x_0\,,\, x_1\,, \ldots, x_m\,)$ tale che, per ogni $\boldsymbol{p}$,

$\boldsymbol{p}$ è primo se e solo se ha soluzione su $\mathbb{N}$ l'equazione $P(\,\boldsymbol{p}\,,\, x_1\,, \ldots,\, x_m\,) = 0\,.$

In maniera piú sbrigativa, utilizzando il teorema di John Wilson[15] secondo cui un numero $p \geqslant 2$ è primo se e solo se p divide $(p-1)! + 1$, otteniamo la seguente specifica della primalità:

$$\mathsf{Primo}\,(p) \quad \leftrightarrow \quad \exists\, k\, \exists\, u\, \big(\quad p \quad = \quad 2 + k \quad \& \quad p\, u \quad = \quad (k+1)! + 1 \quad \big)\,.$$

Un abbellimento di quest'ultima specifica consiste nel caratterizzare la primalità mediante un '*generatore*' della forma $2 + k\, 0^{\mathrm{E}}$, con E espressione a valori positivi.[16] A tale scopo poniamo

$$\mathrm{E}(k,u) \quad =_{\mathrm{Def}} \quad \big((k+1)! - (2+k)\, u + 1\big)^2\,,$$

col che

$$\mathsf{Primo}\,(p) \quad \leftrightarrow \quad \exists\, k\, \exists\, u \qquad p \quad = \quad 2 + k\, 0^{\mathrm{E}(k,u)}\,.$$

I valori che il generatore assume quando le sue variabili spazzano $\mathbb{N}$ sono tutti e soli i numeri primi. Questa specifica ci mostra che la primalità è un predicato esistenzialmente definibile: in effetti, benché $2 + k\, 0^{\mathrm{E}(k,u)}$ non rispetti la sintassi dei polinomi esponenziali (per via, quanto meno, di una sottrazione nell'esponente), non è difficile riscrivere l'equazione $p = 2 + k\, 0^{\mathrm{E}(k,u)}$ come un'equazione i cui membri sono polinomi esponenziali, introducendo nuove incognite che tra l'altro ci permettono di eliminare il fattoriale.

[13] Un tratto originale del citato [Rob52a] è che Julia Robinson, invertendo la consuetudine di formulare il coefficiente binomiale per mezzo del fattoriale, esprime $j\,!$ come quoziente della divisione intera di $\big((2\,j+1)^{2\,j+1}\big)^j$ per il binomiale $\binom{(2\,j+1)^{2\,j+1}}{j}$.

[14] Richiamiamo l'*identità di Bézout*: il massimo comun divisore di due interi N, M con $\{N, M\} \neq \{0\}$ è la piú piccola combinazione lineare positiva $d = I\, N + J\, M$ (con $I, J \in \mathbb{Z}$).

[15] Questo fatto, v. `http://primes.utm.edu/notes/proofs/Wilsons.html` ed `http://www.youtube.com/watch?v=VLFjOP7iFI0`, annunciato da Edward Waring nel 1770, verrà dimostrato da Lagrange poco tempo dopo.

[16] Si tenga presente la comune stipula circa l'esponenziazione, vista come operazione su $\mathbb{N}$:

$$0^m \quad = \quad \left\{ \begin{array}{ll} 1 & \text{se} \quad m = 0\,, \\ 0 & \text{se} \quad m > 0\,. \end{array} \right.$$

Esercizio 19. *Attestare, fissando in modo appropriato i valori di k e di u in* $\mathrm{E}(k,u)$*, che sono veri:* Primo (2)*,* Primo (3) *e* Primo (5)*.*

Il teorema di Matiyasevich rendeva evidente che si poteva proporre, come generatore dei numeri primi, un ordinario polinomio a coefficienti in $\mathbb{Z}$:

> *i valori negativi* (inevitabili) *di un tal generatore polinomiale dovevano semplicemente essere scartati,* come pure lo 0, *mentre i suoi valori positivi sarebbero stati tutti i soli i numeri primi.*

Già nel 1971 Matiyasevich sfruttava in questo senso il proprio teorema, indicando come generare i primi tramite un polinomio in 21 varr., di grado 21 [Mat71].

Riportiamo, adesso, un polinomio rappresentativo dei numeri primi, proveniente da [JSWW76, pag. 449] e piú leggibile sia di quello originario di Matiyasevich che di vari altri susseguitisi negli anni:

$$\left.\begin{aligned}
&(\bullet\, z+h+j-q)^2\\
&+\big((g\,\kappa+2\,g+\kappa+1)\,(h+j)+h-z\big)^2\\
&+(2\,n+p+q+z-e)^2\\
&+\big(16\,(\kappa+1)^3\,(\kappa+2)\,(n+1)^2+1-\bullet^2\big)^2\\
&+\big(e^3\,(e+2)\,(a+1)^2+1-\bullet^2\big)^2\\
&+\big((a^2-1)\,y^2+1-x^2\big)^2\\
&+\big(16\;\bullet^2\;y^4\,(a^2-1)+1-u^2\big)^2\\
&+(n+l+\bullet-y)^2\\
&+\big(\big((a+u^2\,(u^2-a))^2-1\big)\,(n+4\;\bullet\;y)^2+1-(x+\bullet\,u)^2\big)^2\\
&+\big((a^2-1)\,l^2+1-m^2\big)^2\\
&+(a\,i+\kappa+1-l-i)^2\\
&+\big(z+p\,l\,(a-p)\;+\;\bullet\,(2\,a\,p-p^2-1)-p\,m\big)^2\\
&+\big(q+y\,(a-p-1)+\bullet\,(2\,a\,p\;+\;2\,a-p^2-2\,p-2)-\;x\big)^2\\
&+\big(p+l\,(a-n-1)+\bullet\,(2\,a\,n+2\,a-n^2-2\,n-2)-m\big)^2\,.
\end{aligned}\right\}\rightleftharpoons Pr$$

Si tratta di un polinomio Pr in 26 variabili (qui vengono lasciate anonime, designandole con "$\bullet$", quelle che vi figurano una volta in tutto). La variabile κ funge da parametro, mentre le altre—che ora indicheremo come $x_1,\dots,x_{25}$—fungono da 'incognite' in quanto, per ogni $\boldsymbol{\kappa}$ in $\mathbb{N}$,

$\boldsymbol{\kappa}+2$ è primo se e solo se ha soluzione su $\mathbb{N}$ l'eq. $Pr(\,\boldsymbol{\kappa}\,,\,x_1\,,\dots,\,x_{25}\,)=0\,.$

Da Pr a un generatore dei numeri primi il passo è breve, grazie ad un espediente a buon mercato concepito da H. Putnam: generatore è il polinomio

$$(x_0+2)\,\big(\,1-Pr(x_0\,,\,x_1\,,\dots,\,x_{25}\,)\big)\,.$$

Esercizio 20. *Tramutate $Pr(\kappa\,,\,x_1\,,\dots,\,x_{25}\,)$ in un altro polinomio in 26 variabili, che assuma tutti e soli i numeri primi come suoi valori* $\boxed{\geqslant 0}$.

3.5 Risvolti negativi di una soluzione negativa

Poter stabilire la *non-esistenza* di algoritmi che risolvessero particolari problemi, presupponeva che la matematica facesse assoluta chiarezza sul concetto generale di algoritmo: certo non è dovuto al caso che l'esplicitazione di tale concetto e l'individuazione dei primi problemi algoritmicamente insolubili avvengano di pari passo, negli anni 1930. Però né i risultati di Gödel del 1931 né quelli di Church e di Turing del 1936 erano tali da destar sensazione fuori da una ristretta cerchia di logici e di informatici *ante litteram* — Ovvio: chi, all'epoca, poteva prevedere l'imminente rivoluzione tecnologica della *computer science*?

La situazione cambia nel 1947 quando, all'insaputa uno dell'altro, il già citato A. A. Markov in URSS ed Emil L. Post negli USA dimostrano l'insolubilità algoritmica del *problema della parola per i semigruppi*, posto dal norvegese Axel Thue nel 1914: siamo di fronte a un problema 'genuinamente' matematico che, grazie alle nuove metodiche, risulta indecidibile. La risoluzione negativa del X problema di Hilbert costituisce un ulteriore salto di qualità dello stesso segno.

Man mano che i problemi decisionali insolubili vengono meglio circoscritti e diventano piú contigui a problemi tradizionali della matematica, diventa piú facile farne uso per rivelare l'indecidibilità di nuovi problemi: supponiamo che un problema decisionale $\mathfrak{P}$ sia algoritmicamente insolubile e che ogni sua istanza $\mathcal{P}$ sia riducibile a un'istanza $\mathcal{Q}$ di un altro problema decisionale, $\mathfrak{Q}$. Vale a dire, supponiamo di poter facilmente trasformare un responso su $\mathcal{Q}$ in un responso su $\mathcal{P}$. Allora anche $\mathfrak{Q}$ risulta algoritmicamente insolubile.[17]

Impieghi di questo genere del risultato Davis-Putnam-Robinson-Matiyasevich non sono rari. Valga come esempio l'individuazione, da parte di Domenico Cantone, Vincenzo Cutello e Alberto Policriti [CCP90], di frammenti *in*decidibili della teoria degli insiemi; per limitarci a citare uno:

Esempio 21. *La soddisfacibilità delle congiunzioni di vincoli insiemistici nei costrutti della seguente tabella è un problema algoritmicamente insolubile.*

$\bullet \cup \bullet$	UNIONE	(operazione diadica)
$\bullet \times \bullet$	PRODOTTO cartesiano	(operazione diadica)
$\{\bullet\}$	formazione di SINGOLETTO	(operazione monadica)
$\lvert\bullet\rvert$	CARDINALITÀ	(operazione monadica)
$\bullet \cap \bullet = \emptyset$	DISGIUNTEZZA	(predicato diadico)
$\lvert\bullet\rvert \in \mathbb{N}$	FINITEZZA	(predicato monadico)

4 Tre sottoproblemi risolubili del X di Hilbert

4.1 Restrizione del X problema alle equaz. in un'incognita

Un noto teorema dell'algebra rende facile individuare tutte le soluzioni intere $X = \boldsymbol{p}$ di un'equazione della forma $P(X) = 0$, nella sola incognita X, con P

[17] Un'illustrazione di questo metodica è la riduzione del X problema dalla variante riguardante i numeri naturali (dimostrata indecidibile da Davis, Putnam, Robinson e Matiyasevich) alla sua accezione originaria riguardante gli interi, tramite il teor. dei 4 quadrati (vedi § 1.2).

polinomio

$$\boldsymbol{c}_n\, X^n + \boldsymbol{c}_{n-1}\, X^{n-1} + \cdots + \boldsymbol{c}_1\, X + \boldsymbol{c}_0$$

a coefficienti $\boldsymbol{c}_i$ interi. Se $\boldsymbol{c}_0 = 0$, allora una soluzione è $X = 0$ e possiamo semplificare il polinomio. Assumendo dunque, senza perdita di generalità, che $\boldsymbol{c}_0 \neq 0$, $n > 0$ e $\boldsymbol{c}_n \neq 0$, possiamo ricorrere al classico *teor. delle radici razionali*:

> se $P(\,\boldsymbol{p}/\boldsymbol{q}\,) = 0$, dove $\boldsymbol{p}$ è un numero intero, $\boldsymbol{q}$ è un numero naturale e la frazione $\boldsymbol{p}/\boldsymbol{q}$ è ridotta ai minimi termini, allora $\boldsymbol{p}$ divide il termine noto $\boldsymbol{c}_0$ e $\boldsymbol{q}$ divide il coefficiente $\boldsymbol{c}_n$.

Qui a noi interessa solo il caso $\boldsymbol{q} = 1$: per individuare le soluzioni, ci basta dunque passare in rassegna un numero finito di candidati, i divisori interi di $\boldsymbol{c}_0$, e provare a sostituirli alla X.

Esempio 22. *Si candidano a soluzioni dell'equazione*

$$X^3 - 4\,X^2 + 5\,X - 2 \;\;=\;\; 0$$

i quattro divisori di -2*. Due di questi, 1 e 2, effettivamente risolvono l'equazione; gli altri due,* -1 *e* -2*, sono da scartare.*

La dimostrazione del teorema citato, adattata al nostro caso $\boldsymbol{q} = 1$, è semplicissima. Se

$$\boldsymbol{c}_n\, \boldsymbol{p}^n + \boldsymbol{c}_{n-1}\, \boldsymbol{p}^{n-1} + \cdots + \boldsymbol{c}_1\, \boldsymbol{p} + \boldsymbol{c}_0 \;\;=\;\; 0\,,$$

allora

$$\boldsymbol{p}\;\left(\boldsymbol{c}_n\, \boldsymbol{p}^{n-1} + \boldsymbol{c}_{n-1}\, \boldsymbol{p}^{n-2} + \cdots + \boldsymbol{c}_1\right) \;\;=\;\; -\boldsymbol{c}_0\,.$$

Qui l'espressione fra parentesi designa un intero; ovvio, allora, che $\boldsymbol{p}$ divida $\boldsymbol{c}_0$.

4.2 Restrizione del X problema alle equazioni di grado 2

La restrizione del X problema di Hilbert al caso di un'equazione di grado 2 in un numero arbitrario di incognite, è risolubile [Sie72] (vedi anche [Cas08]).

Col grado 4 siamo già nel regno dell'indecidibile (vedi Osservaz. 3), dunque il confine fra istanze decidibili e indecidibili del X problema si situa presso il grado 3. Un'equazione emblematica del 3° grado, studiatissima, è quella in Fig. 11: Mordell ha dimostrato nel 1922 che, per ogni $\boldsymbol{k}$ in $\mathbb{Z} \setminus \{0\}$, questa ha un numero finito di soluzioni su $\mathbb{Z}$. Per quali $\boldsymbol{k}$ càpita che manchino del tutto? Vedi:

`http://oeis.org/A054504`
`http://oeis.org/A081121`

Un classico: l'equazione di Mordell

Claude-Gaspard Bachet de Méziriac (1581–1638)
Louis Joel Mordell (1888–1972)

si appassionarono alla risoluzione dell'equazione

$$Y^2 \;=\; X^3 + k$$

(cosí pure Fermat, per $\underbrace{k=-2 \text{ e } k=-4}_{\text{risolubile}}$; Lebesgue per $\underbrace{k=7}_{\text{irres.}}$).

Figura 11: Per quali valori $\boldsymbol{k}$ del termine noto quest'equaz. ha soluzioni intere?

4.3 Soddisfacibilità di forme normali congiuntive

Definiamo qui due operazioni su un generico dominio d'integrità ordinato:

$$\begin{aligned} \neg x \quad &=_{\text{Def}} \quad (x-1)^2, \\ y \vee z \quad &=_{\text{Def}} \quad y + z - y\,z \end{aligned}$$

(cosicché $x \vee y \vee z \;=\; x\,y\,z - x\,y - x\,z - y\,z + x + y + z$). Consideriamo poi un'equazione della forma

$$\textstyle\sum_{i=1}^{\ell} \neg(\,p_i^2 + \neg p_i\,) + \sum_{j=1}^{\kappa} \neg(\,x_j \vee y_j \vee z_j) \;=\; 0\,, \qquad (*)$$

dove $p_1, \ldots, p_\ell$ sono incognite distinte e

$$\{\,x_1, y_1, z_1, \ldots, x_\kappa, y_\kappa, z_\kappa\,\} \subseteq \{\,p_1, \ldots, p_\ell,\; \neg p_1, \ldots, \neg p_\ell\,\}\,.$$

Nel risolvere l'equazione polinomiale $(*)$ occorre soddisfare ciascuna delle

$$\neg(\,p_i^2 + \neg p_i\,) \;=\; 0\,,$$

in altre parole richiedere che $p_i = 0$ o $p_i = 1$, per ogni i . È chiaro che alle istanze del decimo problema di Hilbert della particolarissima forma $(*)$ (per la cui risoluzione è indifferente che ci si riferisca a $\mathbb{N}$, a $\mathbb{Z}$, a $\mathbb{Q}$, o ad $\mathbb{R}$) si può dare risposta tramite un algoritmo decisionale. Tuttavia rimane un grande problema insoluto dei giorni nostri stabilire se vi sia un algoritmo di complessità polinomiale in grado di rispondere a tutte le istanze di questo tipo (vedi [GJ79]).

Esercizio 23 (Terzo escluso). *Dimostrare che l'equazione* $\neg(\,p^2 + \neg p\,) = 0$ *ha come soluzioni:* $p = 0$, $p = 1$ *e nessun'altra. Quante e quali soluzioni ha*

l'equazione $\neg(\, p \vee \neg p\,) = 0$ *? È risolubile un'equazione della forma* $x \vee y \vee 2 = 1$ *con* $\{x, y\} \subseteq \{p, q, \neg p, \neg q\}$*, se richiediamo che* $\{p, q\} \subseteq \{0, 1, 2\}$*?*

Piú in generale, possiamo definire su sequenze finite di operandi il costrutto 'variadico' $\bigvee$, ponendo:

$$\begin{aligned} \bigvee \langle\, \rangle &=_{\text{Def}} 0\,, \\ \bigvee \langle n_0, n_1, \ldots, n_k\rangle &=_{\text{Def}} n_0 \vee \bigvee \langle n_1, \ldots, n_k\rangle\ , \end{aligned}$$

per $k = 0, 1, 2, \ldots$; considerare, poi, incognite distinte $p_1, \ldots, p_\ell$ e un insieme

$$S \subseteq \mathscr{P}(\{\, p_1, \ldots, p_\ell,\ \neg p_1, \ldots, \neg p_\ell\,\})\,.$$

Rimane vero che all'istanza del X problema di Hilbert riguardante l'equazione[18]

$$\textstyle\sum_{i=1}^{\ell} \neg(p_i^2 + \neg p_i) + \sum_{C \in S} \neg \bigvee C \quad = \quad 0$$

su $\mathbb{N}$ si può dare risposta tramite un algoritmo decisionale che riceve, come suo dato d'avvio, l'insieme S.

Esercizio 24 (**Riduzione di CNF-SAT a 3CNF-SAT (*)**)**.** *Mostrare come il problema di soddisfacibilità proposizionale introdotto nella seconda parte di questo paragrafo possa venire ricondotto a quello presentato nella prima parte.*

Riferimenti bibliografici

[Abb78] James Crawford Abbott, editor. *The Chauvenet Papers,* vol. *2.* Math. Assoc. of America, 1978.

[Cas08] John William Scott Cassels. *Rational Quadratic Forms.* Dover Publications, New York, 2008.

[CCP90] Domenico Cantone, Vincenzo Cutello, and Alberto Policriti. Set-theoretic reductions of Hilbert's tenth problem. In Egon Börger, Hans Kleine Büning, and Michael M. Richter, editors, *CSL '89, 3rd Workshop on Computer Science Logic, Kaiserslautern, Germany, October 2-6, 1989, Proceedings*, volume 440 of *Lecture Notes in Computer Science*, pages 65–75. Springer, 1990.

[CH84] Douglas M. Campbell and John C. Higgins, editors. *Mathematics: People, Problems, Results*, volume 2. Wadsworth International, Belmont, CA, 1984.

[Csi08] George Paul Csicsery. *Julia Robinson and Hilbert's Tenth Problem.* Zala Films, Oakland, CA, 2008. M. Davis, Yu. Matiyasevich and H. Putnam appear in this documentary film, see `http://www.ams.org/ams/julia.html` and `http://www.zalafilms.com/films/juliarobinson.html`.

[18] In quest'equazione le C non sono liste ma insiemi; l'abuso di notazione è perdonabile, in quanto ciascun elemento di $\bigcup S$ assumerà valore 0 oppure 1.

[Dav50] Martin Davis. *On the theory of recursive unsolvability*. PhD thesis, Princeton University, 1950.

[Dav58] Martin Davis. *Computability and Unsolvability*. McGraw-Hill, New York, 1958. Reprinted with an additional appendix, Dover 1983.

[Dav68] Martin Davis. One equation to rule them all. *Transactions of the New York Academy of Sciences. Series II*, 30(6):766–773, 1968.

[Dav71] Martin Davis. An explicit Diophantine definition of the exponential function. *Commun. Pur. Appl. Math.*, XXIV(2):137–145, 1971.

[Dav73] Martin 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* [Dav58, pp. 199–235].

[Dav99] Martin Davis. From logic to computer science and back. In *People & ideas in theoretical computer science*, Series in discrete mathematics and theoretical computer science, pages 53–85. Springer, 1999.

[Dav10] 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.

[DH73] Martin Davis and Reuben Hersh. Hilbert's 10th problem. *Scientific American*, 229:84–91, 1973. Reprinted in [Abb78, pp. 555–571] and in [CH84, pp. 136–148].

[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. Reprinted in [Rob96, p. 269ff.].

[DP59] Martin Davis and Hilary Putnam. A computational proof procedure; Axioms for number theory; Research on Hilbert's Tenth Problem. Technical Report AFOSR TR59-124, U.S. Air Force, October 1959.

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson. The decision problem for exponential Diophantine equations. *Annals of Mathematics, Second Series*, 74(3):425–436, 1961.

[GJ79] Michael R. Garey and David S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. Series of Books in the Mathematical Sciences. W. H. Freeman, 1979.

[Göd31] 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 University Press: 144-195.

[HA28] David Hilbert and Wilhelm Ackermann. *Grundzüge der theoretischen Logik*. Springer-Verlag, 1928. English translation, titled *Principles of Mathematical Logic*, of the 2nd German edition (1938) published by Chelsea Publishing Co., New York, 1950.

[Hil00] David Hilbert. Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker-Kongreß zu Paris 1900. *Nachrichten von der Königliche Gesellschaft der Wissenschaften zu Göttingen*, pages 253–297, 1900.

[Jon82] James P. Jones. Universal Diophantine equation. *The Journal of Symbolic Logic*, 47(3):549–571, 1982.

[JSWW76] 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.

[Kos71] Nikolaj Kirillovič Kosovskiĭ. O Diofantovykh predstavleniyakh posledovatel'nosti reshenii uravneniya Pellya. *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR (LOMI)*, 20:49–59, 1971. (Russian. Available in English translation as [Kos73]).

[Kos73] N. K. Kosovskiĭ. Diophantine representation of the sequence of solutions of the pell equation. *Journal of Soviet Mathematics*, 1(1):28–35, 1973. (Translated from [Kos71]).

[Kre62] Georg Kreisel. A3061: Davis, Martin; Putnam, Hilary; Robinson, Julia. The decision problem for exponential Diophantine equations. *Mathematical Reviews*, 24A(6A):573, 1962.

[Mak77] Gennadij Semenovich Makanin. The problem of solvability of equations in a free semigroup (in Russian). *Mat. Sbornik*, 103:147–236, 1977. English translation in Math. USSR Sbornik 32:129–198, 1977.

[Man77] Yuri Ivanovich Manin. *A course in mathematical logic*. Graduate texts in Mathematics. Springer-Verlag, 1977.

[Mat70a] Ju. V. Matijasevič. Enumerable sets are Diophantine. *Soviet Mathematics. Doklady*, 11(3):354–358, 1970. (Translated from [Mat70b]).

[Mat70b] Yu. V. Matiyasevich. Diofantovost' perechislimykh mnozhestv. *Doklady Akademii Nauk SSSR*, 191(2):279–282, 1970. (Russian. Available in English translation as [Mat70a]; translation reprinted in [Sac03, pp. 269–273]).

[Mat71] Ju. V. Matijasevič. Diophantine representation of the set of prime numbers. *Soviet Mathematics. Doklady*, 12(1):249–254, 1971.

[Mat92] Yuri V. Matiyasevich. My collaboration with Julia Robinson. *The Mathematical Intelligencer*, 14(4):38–45, 1992. (Also available on line at `http://logic.pdmi.ras.ru/~yumat/Julia/`).

[Mat93] Yuri Vladimirovich Matiyasevich. *Hilbert's tenth problem*. The MIT Press, Cambridge (MA) and London, 1993.

[Men97] Elliott Mendelson. *Introduction to Mathematical Logic*. Chapman & Hall, 4$^{\text{th}}$ edition, 1997.

[MR75] Yuri Matijasevič and Julia Robinson. Reduction of an arbitrary diophantine equation to one in 13 unknowns. *Acta Arithmetica*, XXVII:521–553, 1975. Reprinted in [Rob96, p. 235ff.].

[Pea89] Giuseppe Peano. *Arithmetices principia, novo methodo exposita*. Fratres Bocca, Torino, 1889.

[Rob49] Julia Robinson. Definability and decision problems in arithmetic. *The Journal of Symbolic Logic*, 14(2):98–114, 1949.

[Rob52a] Julia Robinson. Existential definability in arithmetic. *Transactions of the American Mathematical Society*, 72(3):437–449, 1952. Reprinted in [Rob96, p. 47ff.].

[Rob52b] Raphael M. Robinson. An essentially undecidable axiom system. In *Proceedings of the International Congress of Mathematicians* (Harvard University, Cambridge, MA, August 30–September 6, 1950), volume 1, pages 729–730. AMS, Providence, RI, 1952.

[Rob69] Julia Robinson. Unsolvable Diophantine problems. *Proc. Amer. Math. Soc.*, 22(2):534–538, 1969.

[Rob72] Julia Robinson. Matiásévič Ú. V. Diofantovost' péréčislimyh množéstv. Doklady Akadémii Nauk SSSR, vol. 191 (1970), pp. 279–282. Matijasevič Ju. V.. Enumerable sets are diophantine. English translation of the preceding by A. Doohovskoy. Soviet mathematics, vol. 11 no. 2 (1970), pp. 354–357. See Errata, ibid., vol. 11 no. 6 (for 1970, pub. 1971), p. vi. *The Journal of Symbolic Logic*, 37(3):605–606, 1972.

[Rob96] 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.

[Sac03] Gerald E. Sacks, editor. *Mathematical Logic in the 20th Century*. Singapore University Press, Singapore; World Scientific Publishing Co., Inc., River Edge, NJ, 2003.

[Sie72] Carl Ludwig Siegel. Zur Theorie der quadratischen Formen. *Nachrichten der Akademie der Wissenschaften in Göttingen. II. Mathematisch-Physikalische Klasse*, 3:21–46, 1972.

[Sko34] Thoralf Skolem. Über die Nicht-charakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschliesslich Zahlenvariablen. *Fundamenta Mathematicae*, 23:150–161, 1934.

[SW95] Daniel Shanks and Samuel S. Wagstaff, Jr. 48 more solutions of Martin Davis's quaternary quartic equation. *Mathematics of Computation*, 64(212):1717–1731, 1995.

[Tar48] Alfred Tarski. A decision method for elementary algebra and geometry. Technical Report R-109, RAND Corporation, Santa Monica, CA, 1948. Prepared for publication with the assistance of J.C.C. McKinsey. Revised 1951, 2nd edition 1957.

[TG08] Terence Tao and Ben Green. The primes contain arbitrarily long arithmetic progressions. *Annals of Mathematics*, 167:481–547, 2008.

[Tur36] A. M. 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 Cenni storici su Diofanto

Chapter II. Diophantine Encoding

Denique fastuosum problema problematum ars Analytice, triplicem Zetetices, Poristices & Exegetices formam tandem induta, jure sibi adrogat, Quod est,
NULLUM NON PROBLEMA SOLVERE.
— *François Viète*

1. Diophantine Equations; Some Background

The main goal of the present chapter is to prove the effective unsolvability of the general problem of deciding which Diophantine equations have solutions. Once we've reached this goal, we will take a look at some applications and refinements. First, however, we must state clearly what the problem involves, i.e., what a Diophantine equation is. That, in part, is the purpose of the present section.

It can be said with confidence that Diophantus of Alexandria lived in Alexandria sometime between the middle of the second century B.C. (since Diophantus mentions a mathematician Hypsikles who lived then) and the middle of the fourth century A.D. (since Theon of Alexandria, who lived then, cites Diophantus). A letter from the eleventh century A.D. asserts that Anatolius of Alexandria (c. middle third century A.D.) had a friend named Diophantus. Moreover, Diophantus dedicated his *Arithmetica* to a "very respected Dionysius" and the best candidate for such an epithet was St. Dionysius, who lived in Alexandria in the third century A.D. Thus, scholars think that Diophantus lived c. 250 A.D.

We are more fortunate when it comes to the work of Diophantus: 6 of the 13 books of his *Arithmetica* have long been preserved and, relatively recently, more was found in Arabic translation. Thus, there is a good enough body of his work for scholars to assess. This assessment has become more positive over the years.

In rough terms, Diophantus posed and solved polynomial equations. As already mentioned in the introductory section of Chapter I, the available notation was rather limited. He had names for one variable and several of its powers. By asserting, for example, that some expression involving this variable and its powers is a square, he was able to express some equations in more than one unknown. Moreover, a felicitous substitution would occasionally reduce the number of variables of an equation to one, allowing Diophantus to handle such equations. For the most part, however, Diophantus treated equations in one variable and he looked for positive rational solutions, generally satisfying himself with producing one solution.

Here, I cannot resist quoting Eric Temple Bell:

C. Smoryński, *Logical Number Theory I*

Diophantus contented himself with special solutions of his problems; the majority of his numerous successors have done likewise, until diophantine analysis today is choked by a jungle of trivialities bearing no resemblance to cultivated mathematics. It is long past time that the standards of Diophantus be forgotten though he himself be remembered with becoming reverence.

Of course, Bell is generally quoted more for the passion of his prose than the soundness of his opinions; but his remark does illustrate an important point: a good method would produce *general* solutions, not merely *specific* solutions. Diophantus is often accused of lacking method. B.L. van der Waerden says simply that Diophantus' method varies from case to case. The historians J.E. Hofmann and O. Becker assert

Diophantus gives no general methods; rather it seems he uses a surprising new trick for each new problem.

A slightly more generous remark is to be found in the *Dictionary of Scientific Biography*:

In only a few cases can one recognize generally applicable methods of solutions in the computations that Diophantus presents, for he considers each case separately, often obtaining a solution by means of brilliant stratagems.

Against this negative tide, I.G. Bashmakova makes a strong case that Diophantus had general methods, later codified during the emergence of algebraic geometry, but that Diophantus simply did not have the notation necessary to make his methods apparent. Supporting this, André Weil says "there is much, in Diophantus and in Viète's *Zetetica*, which in our view pertains to algebraic geometry". [We shall have a look at such a geometric method in section 3, below, when we consider the solutions to the Pythagorean equation,

$$x^2 + y^2 = z^2,$$

and the Pell equation,

$$x^2 - Dy^2 = 1.]$$

For now, I suppose, the lesson to be learned from these remarks is that it requires great sophistication to make something of Diophantus' solutions. The history of things Diophantine prior to Pierre de Fermat as summed up by Fermat's son Samuel (quoted here from Weil's book) reflects this:

Bombelli, in his *Algebra*, was not acting as a translator for Diophantus, since he mixed his own problems with those of the Greek author; neither was Viète, who, as he was opening up new roads for algebra, was concerned with bringing his own inventions into the limelight rather than serving as a torch-bearer for those of Diophantus. Thus, it took Xylander's unremitting labors and Bachet's admirable acumen to supply us with the translation of Diophantus' great work.

Viète, once again, was the man who first introduced the modern variable. His five books of *Zetetica* (1593) are devoted to the algebraic solution of some 30 odd problems from Diophantus. That Viète's solutions are easier to wade through than Diophantus' justifies— for his and (probably) Diophantus' purposes— Viète's thrusting his own inventions into the limelight. Samuel's remark concerned his father's purpose.

Pierre de Fermat read Bachet's edition of Diophantus and discovered something new— number theory. This is not to say that there was a great deal of number theory in Diophantus, but that there was enough to inspire Fermat. The best known example of such