Vincles conceptuals entre els tres problemes metalògics de Hilbert

Josep Pla i Carrera
Professor emèrit de la UB
Magister Honoris Causa per la FME

Jornada Hilbert a l'FME
Facultat de Matemàtiques i Estadística
Universitat Politècnica de Catalunya
Barcelona, 28 de febrer del 2018

David Hilbert

Königsberg (Prússia Oriental), 23 de gener de 1862
Göttingen (Alemanya), 14 de febrer de 1943

1.– Introducció.

David Hilbert, al final de la cèlebre conferència de 1900, *Mathematische Probleme*, en què planteja **vint-i-tres problemes** per tal que siguin resolts al segle xx, diu:

> *La Ciència matemàtica és un tot indivisible, un organisme la força vital del qual té com a condició indispensable la indissolubilitat de les seves parts. Efectivament, sigui quina sigui la diversitat de les matèries de la nostra Ciència en relació amb els detalls, no pot deixar de sorprendre'ns l'equivalència dels processos lògics, el parentesc que hi ha entre las idees en el conjunt de la Ciència i també nombroses analogies en els diferents dominis. Observem, encara, el fet següent: Com més es desenvolupa una teoria matemàtica, més guanya la seva exposició en harmonia i en unitat, i descobrim relacions entre aquesta teoria i les branques de la Ciència que fins aleshores li eren alienes. Així, encara que la Matemàtica estengui els dominis, mai no perd el caràcter unitari sinó que, al contrari, se'ns ofereix cada cop d'una manera més evident.*

D'acord amb un paràgraf anterior:

> *Sovint, la raó per la qual no aconseguim resoldre un problema matemàtic és que no hem assolit un punt de vista prou general des del qual el problema se'ns mostra com una simple baula d'una cadena de problemes de la mateixa naturalesa. Però quan assolim aquest punt de vista, no només el problema es fa més abordable, sinó que a més ens trobem en possessió d'un mètode aplicable als problemes de la mateixa espècie.*

Objectiu de l'exposició. Establir els nexes conceptuals que permeten relacionar, encara que només sigui des del vessant conceptual de la lògica, tres dels coneguts problemes de Hilbert —els metalògics.

El concepte de **recursivitat enumerable**, convenientment adaptat a cada problema particular, proporciona un nexe conceptual d'aquests problemes.

▶ 4
▶ 15

Problema 1. *Demostrar que només hi ha dos conjunts de nombres equivalents: el numerable i el continu.*

Problema 2. *Demostrar que els axiomes no són contradictoris; és a dir, que, basant-nos en els axiomes i amb un nombre finit de deduccions lògiques, mai no obtindrem resultats contradictoris.*

Problema 10. *Trobar un mètode que, amb un nombre finit d'operacions, permeti decidir si una equació arbitrària [de Diofant] és resoluble en els món dels nombres enters racionals.*

En la mentalitat de Hilbert, donat un problema matemàtic, s'ha d'establir una **teoria axiomàtica** "ad hoc" —és a dir, adequada per a la seva resolució. I, un cop establerta, l'hem de resoldre al seu si.

> *Aquest axioma —***la possibilitat de resoldre qualsevol problema***—, ¿és una propietat característica i distintiva del pensament matemàtic? ¿O és una llei general de la manera de procedir del nostre enteniment? O sigui, ¿el nostre enteniment pot resoldre totes les qüestions que es planteja?* [...]
>
> [...] *Hi ha problemes que finalment s'han resolt satisfactòriament establint-ne la impossibilitat, i, malgrat aquesta circumstància, han estat de la màxima utilitat en el desenvolupament de la Ciència.*

Però hi ha més. **Cap veritat** no pot quedar exclosa.

> *En el nostre quefer quotidià, la possibilitat de resoldre un problema matemàtic, el que sigui, és un preciós incentiu que, en tot moment ressona, al nostre interior:*
>
> > *Heus aquí el problema. Busquem-li la solució. Pots trobar-la per mitjà del raonament pur. Efectivament, cap matemàtic es veurà mai reduït a haver que dir: «***Ignorabimus***».*

La xerrada la plantegem en el context que Hilbert imposa en el *Mathematische Probleme* [1900]:

> El context en el qual s'han de resoldre els problemes matemàtics són els sistemes axiomàtics «ad hoc».
>
> Aquests sistemes han de satisfer tres propietats:
>
> 1) No hi ha **Ignorabimus**.
> 2) Han de ser **decidibles**.
> 3) Han de ser **consistents**.

Abans, però, calia precisar el context lògic en el qual expressar les teories axiomàtiques. Es trigarien trenta anys:

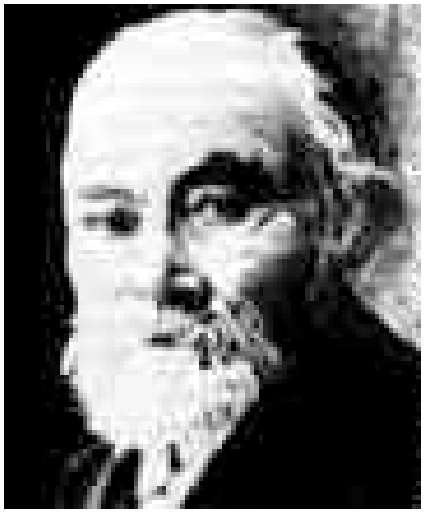
> **Context lògic** Una teoria axiomàtica, en el sentit hilbertià, s'ha de fonamentar en la lògica de predicats de primer ordre, amb igualtat.

2.– Les fites dels antecedents històrics. Els problemes de Hilbert esmentats —i la seva resolució— són metamatemàtics.

El primer, fa referència a la teoria de conjunts de Cantor de primer ordre; el segon, en canvi, a l'aritmètica de Peano de primer ordre.

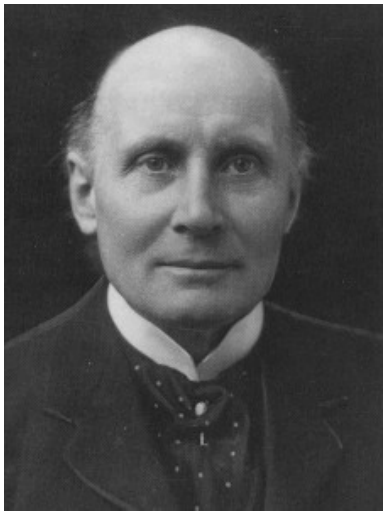
Val la pena recordar algunes fites del context històric:

Georg Cantor
(1845-1918)



Gottlob Frege
(1848-1925)

Giuseppe Peano
(1858-1932)



Alfred North Whitehead
(1861-1947)

Erns Zermelo
(1871-1953)

Bertrand Russell
(1872-1970)

Thoralf Skolem
(1887-1963)

Wilhelm Ackermann
(1896-1962)

Leopold Löwenheim (1878-1957)

1877 Gottlob Frege i el *Begriffsschrift*: connectives lògiques i quantificadors sobre variables de primer ordre [i superiors].

1879 Georg Cantor inicia l'estudi de la naturalesa dels conjunts i la seva mida ordinal i cardinal.

1888 Giuseppe Peano dona l'axiomàtica de l'aritmètica dels nombres naturals amb l'axioma d'inducció conjuntista.

1899 David Hilbert i l'axiomàtica de la geometría euclidiana: tres menes de variables i amb axiomes d'ordre superior.

1900 David Hilbert i l'axiomàtica de l'aritmètica dels nombres reals amb l'axioma de completitud conjuntista.

1908 Erns Zermelo i l'$\surd axiomàticadelateoriadeconjuntsdeCantor$: $elconceptedepro-pietat$**no**$estàclar$.

1910/13 Alfred North Whitehead y Bertrand Russell publiquen *Principia Mathematica*: text fundacional de la lògica matemàtica d'ordre superior.

1915 Leopold Löwenheim estableix que tota sentència vàlida té un model numerable. Neix la teoria de models.

1917 *Lliçons de lògica* de Hilbert: considera la lògica de primer ordre com un subsistema lògic propi i planteja dues qüestions relatives a aquest subsistema:

1) La completesa.
2) La decidibilitat (L'**Entscheidungsproblem**).

1920 Thoralf Skolem extén el resultat de Löwenheim a famílies de sentències.

1923 Thoralf Skolem dona l'axiomàtica de **red**primer ordre de la teoria de conjunts de Cantor. Estableix el concepte de **propietat ben definida** en el llenguatge lògic $\mathsf{L}_{\mathsf{con}}$.

És el context en el qual es planteja el problema 1: $\vdash_{\mathbf{ZF}} 2^{\aleph_0} = \aleph_1$?

1925 Hilbert confirma la teoria de la demostració. Estableix l'**axiomàtica de la lògica de primer orden amb igualdad**. És el substracte lògic general. ◀ 1

1928 Hilbert dona l'axiomàtica de la aritmètica de Peano en primer ordre.

És el context en el qual es planteja el problema 2: $\vdash_{\mathbf{P}} \mathtt{Consist}_{\mathbf{P}}$? ◀ 1

Hilbert i Wilhelm Ackermann publiquen el text fundacional de la lògica en el sentit de Hilbert —la lògica del **formalisme**: *Grundzüge der theoretischen Logik*. [S'hi recullen les lliçons de 1917.]

1929 Kurt Gödel estableix la **completesa** de la lògica de primer ordre que lliga veritat **semàntica** i **sintàctica**.

Una propietat molt important. En l'aritmètica de Peano ($\mathbf{P}$) i en la teoria de conjunts de Cantor ($\mathbf{ZF}$ o $\mathbf{ZFC}$), de primer orden, les fórmules $\varphi(v_1)$ amb una variable libre v_1 estableixen les propietats, que les podem pensar com a subconjunts definibles.

Així doncs, **formalment** —des de la teoria $\mathbf{P}$—, $\mathbb{N}$ només té una infinitat **numerable** de subconjunts definibles. I l'axioma d'inducció es redueix a ells.

A la teoria de conjunts ($\mathbf{ZF}$), l'axioma d'especificació estableix que cada conjunt X té una quantitat **numerable** de subconjunts definibles.

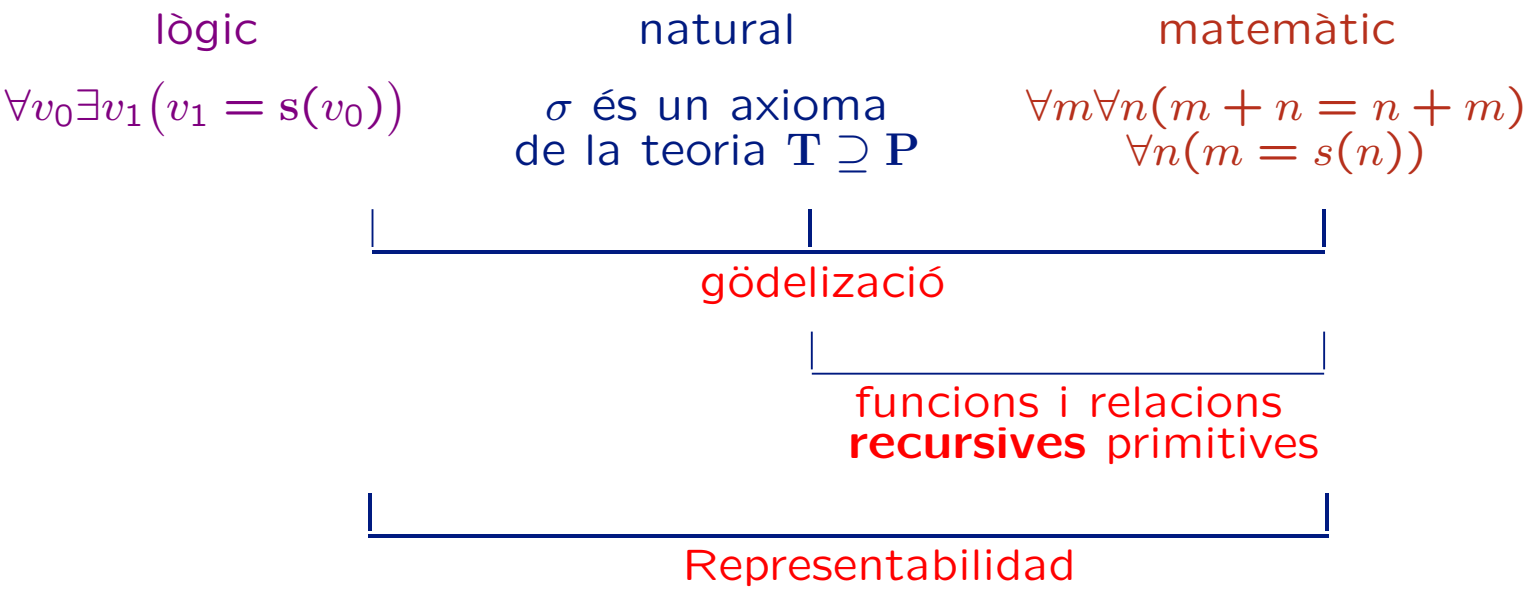
▶ 10

Kurt Gödel

Brno (Imperi Austrohongarès, avui República Txeca), 28 d'abril de 1906
Princeton (New Jersey, Estats Units d'Amèrica), 14 de gener de 1978

3.– El Ignorabimus i l'Entscheidungsproblem.

1931: A "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme", Kurt Gödel analitza la connexió que hi ha entre els **tres** llenguatges implicats en tot procés de raonament lògic de l'aritmètica de Peano dels nombres naturals. Són:



Sigui $\mathbf{P} \subseteq \mathbf{T} \subseteq \mathrm{Pred}(\mathbf{L})$ una extensió consistent de l'aritmètica de $\mathbf{P}$ de Peano, amb $\mathbf{L} \supseteq \mathbf{L}_{\mathrm{ar}}$, en què les relacions recursives són representables.

Definició 3.1. Per a cada $\alpha(v_1) \in \mathrm{Pred}(\mathbf{L})$, sigui $\mathbb{N}_\alpha = \{k \in \mathbb{N} : \vdash_{\mathbf{T}} \alpha(\mathbf{k})\}$.

▶ És a dir, $k \in \mathbb{N}_\alpha$ si, i només si, existeix una $\mathbf{T}$-demostració $\alpha_1, \ldots, \alpha_r$ de $\alpha(\mathbf{k})$.

Es tradueix en una relació ternària de nombres naturals:

$m = \mathrm{god}\big(\alpha_1, \ldots, \alpha_r\big)$, $n = \mathrm{god}\big(\alpha(v_1)\big)$ i k arbitrari.

Definició 3.2. Considerem la relació ternària $W_{\mathbf{T}} \subseteq \mathbb{N}^3$:

$W_{\mathbf{T}}(m, n, k)$ si, i només si, m, n, k satisfan el que hem dit.

▶ $W_{\mathbf{T}}(m, n, k) := Dem_{\mathbf{T}}\big(m, Subst\big(n, k_1, Num(k)\big)\big)$, en què $Dem_{\mathbf{T}}$ és la relació binària $Dem_{\mathbf{T}}(m, n)$ si, i només si, m és el número de Gödel d'una $\mathbf{T}$-demostració de la fórmula de número n i Num i $Subst$ són una funció monària i una ternària, respectivament, recursives primitives i $k_1 := \mathrm{god}(v_1)$.

És obvi que

Lema. Fixem $n = \mathrm{god}\big(\alpha(v_1)\big)$. $\mathbb{N}_\alpha = \{k \in \mathbb{N} : \vdash_{\mathbf{T}} \alpha(\mathbf{k})\} = \exists m\, W_{\mathbf{T}}(m, n, k) := R(n, k)$.

Si alliberem n, tenim la relació binària $R(n, k) \subseteq \mathbb{N}^2$

▶ 10

Proposició de Gödel. La relació recursiva primitiva $W_{\mathbf{T}}$ és $\mathbf{T}$-representable.

És a dir, existeix una fórmula $\mathtt{W}(v_3, v_2, v_1)$ de Pred($\mathbf{L}$) de manera que

$$\vdash_{\mathbf{T}} \mathtt{W}(\mathbf{m}, \mathbf{n}, \mathbf{k}), \text{ si } \langle m, n, k\rangle \in W_{\mathbf{T}};$$
$$\vdash_{\mathbf{T}} \neg\mathtt{W}(\mathbf{m}, \mathbf{n}, \mathbf{k}), \text{ si } \langle m, n, k\rangle \notin W_{\mathbf{T}}.$$

▶ 13

Fem: $\mathtt{W}_1(v_2, v_1) := \mathtt{W}(v_2, v_1, v_1)$, $\gamma(v_1) := \forall v_2 \neg \mathtt{W}_1(v_2, v_1)$ i $\gamma(\mathbf{n}) := \forall v_2 \neg \mathtt{W}_1(v_2, \mathbf{n})$.

▶ 11

Aquestes fórmules són molt importants en la teoria de Gödel.

Gödel i altres autors estableixen l'**equivalència** entre conjunt recursiu i conjunt representable, i anàlogament entre les relacions i les funcions.

Proposició 3.1. Tot conjunt recursiu A és de la forma $\mathbb{N}_\alpha$.

- Només cal considerar una de les fórmules $\alpha(v_1)$ que $\mathbf{T}$-representen al conjunt A.

En conseqüència, hi subconjunts de $\mathbb{N}$ que no són recursius.

◀ 5

En podem identificar algun?

Proposició 3.2. El conjunt $U = \{k \in \mathbb{N} : \neg R(k, k)\}$ no és recursiu.

- Si ho és, existeix $\alpha(v_1)$, amb $n = \text{god}\big(\alpha(v_1)\big)$, i $U = \mathbb{N}_\alpha = R(n, k)$.
  Què passa amb aquest n?
  $n \in U$ si, i només, si $\neg R(n, n)$ i
  $n \in U$ si, i només, si $n \in \mathbb{N}_\alpha$ si, i només si, $R(n, n)$.

◀ 6

U **no és** representable sintàcticament, però **ho és** semànticament.

Proposició 3.3. $n \in U$ si, i només si, $\models_{\mathbb{N}} \gamma(\mathbf{n})$.

- Consecuencia inmediata de las definiciones dadas.

◀ 9

Teorema 3.1. Si $\mathbf{T}$ és consistent, existeix un $n \in \mathbb{N}$ i

$$\models_{\mathbb{N}} \gamma(\mathbf{n}) \quad \text{i} \quad \nvdash_{\mathbf{T}} \gamma(\mathbf{n}).$$

Per tant, tenim el **teorema d'incompletesa de Gödel** en base al de completesa:

$$\nvdash_{\mathbf{T}} \neg\gamma(\mathbf{n}) \text{ i } \nvdash_{\mathbf{T}} \gamma(\mathbf{n}).$$

- $\mathbb{N}_\gamma \subsetneq U$.

◀ 8

En honor a Gödel, fem $\sigma_{\mathsf{G}} := \gamma(\mathbf{n})$. És fàcil demostrar que $k_\gamma = \mathsf{god}\big(\gamma(v_1)\big)$ és un d'aquests n.

Hi ha teories formals de primer ordre amb **Ignorabimus**: No necessàriament **completa**.

- **Ignorabimus.** Hem demostrat que, a $\mathbf{T}$, hi ha veritats que no són demostrables. Per tant no tot allò que és vertader és demostrable. És a dir, es dona Ignorabimus.

Queda pendent l'Entscheidungsproblem: $\mathbf{T}$ és decidible?

Alan Mathison Turing

Paddington (Londres, Anglaterra),
23 de juny del 1912
Wilmslow (Cheshire, Anglaterra),
7 de juny del 1954

Alonzo Church

Washington, D.C. (USA),
14 de juny del 1903
Hudson (Ohio, USA),
11 d'agost de 1955

1936: Alan Turing i Alonzo Church, independentement, donen la definició de *funció computable* i, de retruc, de *conjunt decidible*.

Definició 3.3. A és *decidible* si, i només si, 1_A és *computable*.

A més, Church estableix la **tesi de Church**:

En el món de les funcions de nombre enters positius, identifiquem les nocions efectivament computable, suara discutida, i recursiva o de λ-definible d'enters positius. Crec que aquesta definició està justificada per les consideracions que exposo tot seguit i pel fet de que mai serem capaços de donar una justificació positiva elegint una definició formal que correspongui a una noción intuïtiva.

En concret, un conjunt A és decidible si, i només si, és recursiu.

Teorema 3.2. Existeix un subconjunt de $\mathbb{N}$ que **no** és decidible.

- És el conjunt U.

Per tant,

Teorema 3.3. La relació $Teor_{\mathbf{T}}(n) := \exists m\, Dem_{\mathbf{T}}(m,n)$ **no** és decible.

- $n \in U$ si, i només si, $\neg Teor_{\mathbf{T}}\big(Subst\big(n, k_1, Num(n)\big)\big)$.

En definitiva,

Decidibilitat. Hem demostrat que hi ha teories, en particular la teoría $\mathbf{P}$, que **no** són decidibles.

Emil Leon Post

Augustów (Suwałki Governorate, Imperi Rus, ara Polònia), 21 d'abril de 1954

Nova York (USA), 21 d'abril de 1954

1944: En estudiar l'Entscheidungsproblem, Emile Post introdueix els conjunts recursivament enumerables.

Definició 3.4. Un conjunt E és recursivamente enumerable [r.e.] si, i només si, és de la forma

$$\exists m\, R(m,n),$$ en què relació binària $R(m,n)$ és recursiva.

És posible establir les equivalències següents, que podem considerar com a possibles definicions:

- Un conjunt A és recursiu si, i només si, 1_A és una funció recursiva.
- Un conjunt E és recursivament enumerable [r.e.] si, i només si, $R = \mathrm{Im} f$, en què f és una funció recursiva.

És evident que

Proposició de Post. El conjunt $T = \neg U = Teorema_{\mathrm{T}}(n) {:=} \exists m\, Dem_{\mathrm{T}}(m,n)$ és r.e., pero **no** és recursiu.

- Això és un corol·lari del teorema següent: Un conjunt A és recursiu si, i només si, A i $\neg A$ son r.e.

En definitiva, tenim que

- $T = \neg U$ és r.e., pero no és recursiu.
- U **no** és ni r.e. **ni** recursiu.

Ens plantejàvem un objetiu clar: Trobar un concepte que unifiqui els tres problemes esmentats.

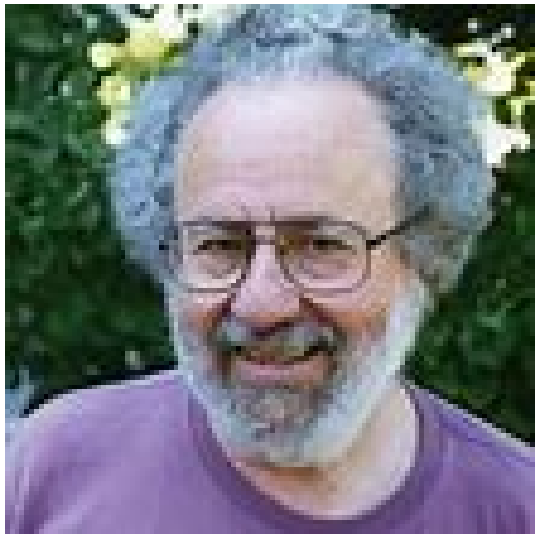
◀ 2

Tesi. Com veurem tot seguit, he trobat que la **recursividad enumerable**, convenientment adaptada a cada problema concret de Hilbert és un nexe.

Gödel en 1931 i Post a 1944 van establir les relacions entre els conjunts (i les relacions) recursius i r.e. i les operacions lògiques:

operación lógica en els conjunts	conjunts recursius	r.e.	diofàntics
$\neg$	sí	no	no
$\wedge$	sí	sí	sí
$\vee$	sí	sí	sí
$\exists u \leq v$	sí	sí	sí
$\forall u \leq v$	sí	sí	?
$\exists u$	no	sí	sí
$\forall u$	no	no	no

▶ 16



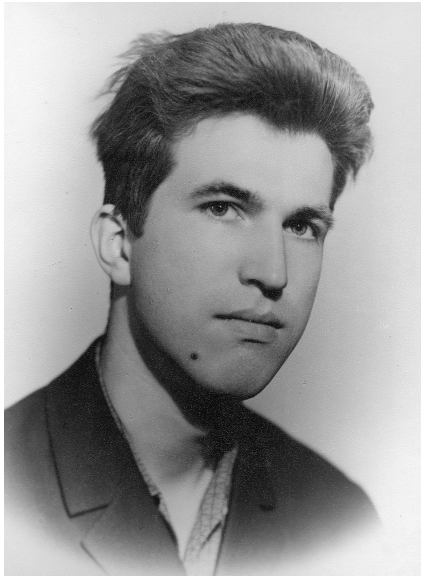
Martin David Davis

Nova York, 1928

Julia Bowman Robinson

Sant Louis (Missouri, USA),
8 de desembre del 1919

Oakland (Califòrnia, USA),
30 de juliol del 1985



Yuri Matijasevicz

Leningrad (Unió Soviètica)
2 de març del 1947

4.– El Entscheidungsproblem i el problema diofàntic.

1934: Gödel relaciona el primer teorema d'incompletesa amb la resolubilitat de certes equacions polinòmiques.

Hi ha una afirmació sobre les solucions d'una equació diofàntica que **no** *és decidible en el nostre sistema formal.* [...] *És a dir, sobre la base dels principis deductius matemàtics actuals,* **no** *hi pot haver cap teoria completa de l'anàlisi diofàntica, ni d'un problema de la forma* $\pi(Q = 0)$.

1950: Davis dona els primers passos.

Definició 4.1. Un conjunt D és diofàntic si, i només si, existeix un polinomi $P(X_0, X_1, \ldots, X_m) \in \mathbb{Z}[X_0, X_1, \ldots, X_n]$ que satsifà

$n \in D$ si, i només si, $P(n, X_1, \ldots, X_m) = 0$ té solucions enteres positives.

- Val també per a relacions ℓ-àries, $R(n_1, \ldots, n_\ell)$. Els polinomios són de $\mathbb{Z}(Y_1, \ldots, Y_\ell, X_1, \ldots, X_m)$.

Teorema de la forma normal de Davis. Tot conjunt E r.e. és de la forma

$n \in E$ si, i només si, $\exists y \forall k \leq y P(n, y, k, X_1, \ldots, X_m) = 0$ té solucions a $\mathbb{Z}_+$.

Conseqüència. Si les relacions diofàntiques estan tancades per quantificació universal afitada (?), els conjunts diofàntics i els conjunts r.e. coinciden.

1952: J. Robinson introdueix els conjunts exponencial diofàntics i demuestra que coincideixen con els conjunts r.e.

Definició 4.2. Un conjunt ED és exponencial diofàntic si, i només si, existeix un polinomi $P(X_0, X_1, \ldots, X_m)$ de manera que

$n \in ED$ si, i només si, $P(n, x_1^{y_1}, \ldots, x_m^{y_m}) = 0$ té solucions a $\mathbb{Z}$

- Esto vale también para relaciones ℓ-arias.

Teorema de J. Robinson. Els conjunts exponencial diofàntics i els r.e. coincideixen.

- Val també per a relacions.

Objetiu. Demostrar que la funció exponencial $w = u^v$ és diofàntica, ja que implicaria que els conjunts r.e. i els diofàntics coincidissin.

I dona una condició suficient per tal que això passi:

Condición suficiente de J. Robinson. Per tal que les funcions exponencial diofàntiques siguin diofàntiques, **és suficient** l'existència d'**una** relació diofàntica $D(u, v)$ de manera que

1) $D(u, v)$ implica $v \leq u^u$.
2) Per a tot, k existeix una parella u, v, amb $v > u^k$, que satisfà $D(u, v)$.

Com dèiem, tot es redueix a veure que la funció exponencial $w = u^v$ és diofàntica. Només cal, doncs, trobar relació $D(u, v)$ una que compleixi la condició de J. Robinson.

1971: Matijasevicz estableix el teorema

Teorema de Matijasevicz. La condición de J. Robinson és verdadera.

- El conjunt $D = \{\langle u, v\rangle : v = a_{2u} \wedge u \geq 2\}$, en què a_i són els nombres de la sucecssió de Fibonacci $a_0 = a_1 = 1, a_{i+2} = a_i + a_{i+1}$, la satisfà.

Així queda establert definitivament el problema deu de Hilbert:

Problema deu de Hilbert. **No** existeix cap algorisme que permeti decidir si una equació diofántica arbitrària és resoluble en $\mathbb{N}$.

- S'enumeren els polinomis mab una gödelització recursiva g. Es considera el conjunt

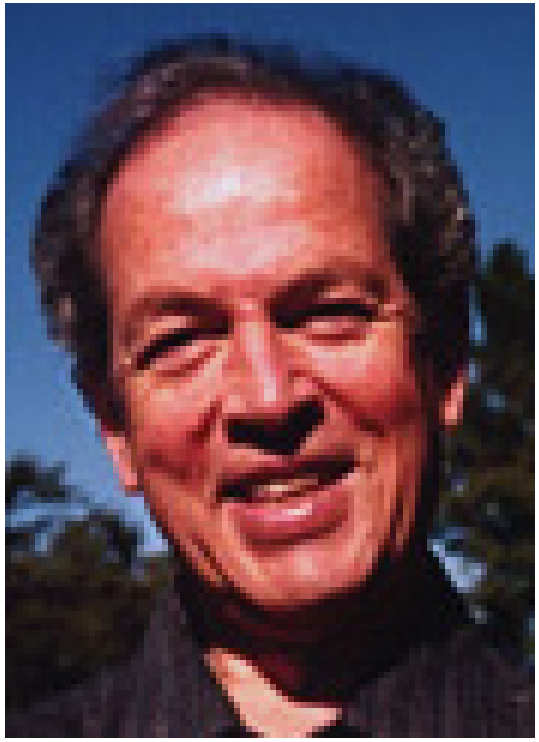
$$H = \big\{n \in \mathbb{N} : P(X_1, \ldots, X_m) = 0 \text{ té solució en } \mathbb{N}\big\}, \text{ en què } n = \text{god}\big(P(X_1, \ldots, X_m)\big).$$

Ara considerem el conjunt r.e., però no recursiu, $T = \neg U$. Existeix un polinomi $Q(X_0, X_1, \ldots, X_m)$ que defineix T.

Així doncs, $n \in T$ si, i només si, $Q_n(X_1, \ldots, X_m) = 0$ té solució a $\mathbb{N}$, en què $Q_n(X_1, \ldots, X_m) := Q(n, X_1, \ldots, X_m)$.

Per tant, $n \in T$ si, i només si, $g\big(Q_n(X_1, \ldots, X_m)\big) \in H$. O sigui, $1_T = 1_H \circ g$.

En definitiva, H **no** és decidible porqué la funció 1_T **no** és recursiva.



Solomon Feferman

Nova York (USA),
13 de desembre del 1928

Stanford (Califòrnia, USA),
26 de juliol del 2016

?

Joseph R. Shoenfield

Detroit (USA), 1927

Durham (North Carolina, USA)
15 de novembre del 2000

5.– El segundo problema de Hilbert.

1931: Gödel afirma que **és possible** refer tots els raonaments metalògics de la demostració del teorema d'incompletesa al si del sistema formal $\mathbf{T}$ i demostrar que

$$\vdash_{\mathbf{T}} \mathtt{Consist}_{\mathbf{T}} \to \sigma_G.$$

Però sabem que, si $\mathbf{T}$ és consistent, $\nvdash_{\mathbf{T}} \sigma_G$.

Per tant, si $\mathbf{T}$ és consistent, $\nvdash_{\mathbf{T}} \mathtt{Consist}_{\mathbf{T}}$.

▶1939: Hilbert i Paul Bernays van proporcionar la primera demostració del teorema, usant les condicions de Löb de la fórmula

$$\tau(v_1) := \exists v_2 \delta(v_2, v_1),$$

en què $\delta(v_2, v_1)$ representa la relació recursiva primitiva $Dem_{\mathbf{T}}(m, n)$. ◀ 8

▶1960: Solomon Feferman estudia en profunditat quines són les condicions que permeten garantir que és impossible demostrar la consistència d'una teoria al si de la pròpia teoria.

Observa que, si $Ax_{\mathbf{T}}(n)$ és representable amb una fórmula
—recursivament enumerable, **no** és possible demostrar la consistència de $\mathbf{T}$ dins de $\mathbf{T}$.
—recursiva, **és** possible demostrar-la.

Les fórmules adequades per a poder traslladar dins la teoria $\mathbf{T}$ els arguments de la metateoria són les fórmules **re**.

Definició 5.1. Les fórmules **re** de Pred($\mathbf{L}$) es defineixen recursivament per:

1) $w = \mathbf{f}v_1 \cdots v_k$, $\mathbf{r}v_1 \cdots v_k$, $\neg\mathbf{r}v_1 \cdots v_k$ són fórmules **re**.
2) Si α i β ho són, $\alpha \wedge \beta$ i $\alpha \vee \beta$ també.
3) Si $\alpha(v)$ ho és, $\forall v \leq w\, \alpha(v)$ també.
4) Si $\alpha(v)$ ho és, $\exists v\, \alpha(v)$ també.
5) No n'hi ha més.

◀ 15

Les fórmules re tenen propietats importants. ▶ 18

Proposició 5.2. Tenim les propietats següents:

a) $w = t, t \in$ Term($\mathbf{L}$) és $\mathbf{T}$-equivalent a una fórmula re de Pred($\mathbf{L}_{\text{ar}}$).
b) Tota fórmula oberta de Pred($\mathbf{L}$) és $\mathbf{T}$-equivalent a una fórmula re de Pred($\mathbf{L}_{\text{ar}}$).
c) Tota fórmula existencial de Pred($\mathbf{L}$) és $\mathbf{T}$-equivalent a una fórmula re de Pred($\mathbf{L}_{\text{ar}}$).
d) Tota fórmula re de Pred($\mathbf{L}$) és $\mathbf{T}$-equivalent a una fórmula re de Pred($\mathbf{L}_{\text{ar}}$).

▶ 21

▶ Totes les demostracions es fan per inducció sobre la complexidad de la fórmula.

Un teorema notable.

La validesa en el model $\mathbb{N}$ [$\models_{\mathbb{N}}$] implica la $\mathbf{P}$-demostrabilitat [$\vdash_{\mathbf{P}}$].

Teorema 5.3. Tota instància numèrica **verdadera** —vàlida en $\mathbb{N}$— d'una fórmula re de Pred($\mathbf{L}_{\text{ar}}$) és un $\mathbf{P}$-teorema.

- Por inducción sobre la complejidad de la fórmula.

Teorema de Shoenfield. Tota sentència existencial de Pred($\mathbf{L}$), vàlida en $\mathbb{N}$, és un $\mathbf{T}$-teorema.

- Por inducción sobre la complejidad de la fórmula.

Recordem el teorema 3.1 i que la fórmula $\gamma(v_1) := \forall v_2 \neg \mathtt{W}_1(v_2, v_1)$ ◀ 12 és, de fet, $\forall v_2 \neg \mathtt{Dem}_{\mathbf{P}}\big(v_2, \mathtt{Subst}\big(v_1, k_1, \mathtt{Num}(v_1)\big)\big)$, en què $\mathtt{Dem}_{\mathbf{P}}$, $\mathtt{Subst}$, $\mathtt{Num}$ ◀ 9 ◀ 7 representen, respectivament, $Dem_{\mathbf{P}}$, $Subst$, Num.

Hipòtesi auxiliar. La sentència $\neg\gamma(\mathbf{n}) := \exists v_2 \mathtt{Dem}_{\mathbf{P}}\big(v_2, \mathtt{Subst}\big(\mathbf{n}, k_1, \mathtt{Num}(\mathbf{n})\big)\big)$ és existencial.

Aleshores, per 5.2 c, existeix una sentència re de Pred($\mathbf{L}_{\text{ar}}$), σ_γ, per ◀ 17 a la qual $\vdash_{\mathbf{T}} \neg\gamma(\mathbf{n}) \longleftrightarrow \sigma_\gamma$.

La dificultat rau a saber si això es pot aconseguir a la teoria $\mathbf{P}$ i amb el llenguatge $\mathbf{L}_{\text{ar}}$ (vegeu la pàgina 28).

Tenim les eines per refer la demostració del teorema de incompletesa de Gödel:

Raonament metalògic del teorema de incomplesa de Gödel.

◀ 17

Raonament metalògic.

1) $\models_{\mathbb{N}} \neg\gamma(\mathbf{n})$ implica $\models_{\mathbb{N}} \sigma_\gamma$.
2) $\models_{\mathbb{N}} \sigma_\gamma, \sigma_\gamma$ re de $\mathrm{Pred}(\mathbf{L}_{\mathrm{ar}})$. Per el teorema 5.2 c, $\vdash_{\mathbf{P}} \sigma_\gamma$.
3) Per la hipòtesi auxiliar, $\neg\gamma(\mathbf{n})$ és existencial a $\mathbf{L}$. Per tant, $\vdash_{\mathbf{P}} \neg\gamma(\mathbf{n})$.
1′) $\not\models_{\mathbb{N}} \gamma(\mathbf{n})$. Aleshores, $n \notin U$. Per tant, $R(n,n)$ i, de retruc, $\vdash_{\mathbf{P}} \gamma(\mathbf{n})$.
4) De 1) i 1′), si $\not\models \gamma(\mathbf{n})$, tenim $\vdash_{\mathbf{P}} \neg\gamma(\mathbf{n})$ i $\vdash_{\mathbf{P}} \gamma(\mathbf{n})$.
   Per tant, $\mathbf{P}$ és inconsistent.
5) En conseqüència, si $\mathbf{P}$ és consistent, $\models \gamma(\mathbf{n})$.

La rèplica dins la teoria formal.

▶ 22

Demostración formal.

1) $\vdash_{\mathbf{P}} \neg\gamma(\mathbf{n}) \longrightarrow \sigma_\gamma$.
2) $\vdash_{\mathbf{P}} \sigma_\gamma \longrightarrow \mathtt{Teorema}_{\mathbf{P}}(\mathbf{c})$, en què $c = \mathrm{god}(\sigma_\gamma)$.
3) $\vdash_{\mathbf{P}} \mathtt{Teorema}_{\mathbf{P}}(\mathbf{c}) \longrightarrow \mathtt{Teorema}_{\mathbf{P}}(\mathtt{Neg}(\mathbf{a}))$, en què $a = \mathrm{god}(\gamma(\mathbf{n}))$.
1′) $\vdash_{\mathbf{P}} \neg\gamma(\mathbf{n}) \longrightarrow \mathtt{Teorema}_{\mathbf{P}}(\mathbf{a})$.
4) $\vdash_{\mathbf{P}} \mathtt{Teorema}_{\mathbf{P}}(\mathbf{a}) \wedge \mathtt{Teorema}_{\mathbf{P}}(\mathtt{Neg}(\mathbf{a})) \longrightarrow \neg\mathtt{Consist}_{\mathbf{P}}$.
5) $\vdash_{\mathbf{P}} \mathtt{Consist}_{\mathbf{P}} \longrightarrow \gamma(\mathbf{n})$ i sabem que $\nvdash_{\mathbf{P}} \gamma(\mathbf{n})$.
   Per tant, $\nvdash_{\mathbf{P}} \mathtt{Consist}_{\mathbf{P}}$, tal com volíem.

▶ Per garantir que $\neg\gamma(\mathbf{n})$ és existencial hem de recórrer a les extensions (definicionals) recursives:
Per a cada funció i relació recursiva de la demostració metalògica del teorema de incompletesa de Gödel, introduïm un símbol funcional o predicatiu de la mateixa arietat. Així per exemple, introduïm el símbol predicatiu binari $\mathbf{Dem_P}$ i els funcionals monaris $\mathbf{Num}$ i $\mathbf{Neg}$ i ternari $\mathbf{Subst}$.
Obtenim un llenguatge $\mathbf{L}$ i una teoria $\mathbf{T}$ que estenen consistentement $\mathbf{L}_{\text{ar}}$ i $\mathbf{P}$.
En ells, hi ha la sentència existencial

$$\neg\gamma^*(\mathbf{n}) := \exists v_2\, \mathbf{Dem_P}\Big(v_2, \mathbf{Subst}\big(\mathbf{n}, \mathbf{k}_1, \mathbf{Num}(\mathbf{n})\big)\Big).$$

Per 5.2 c, li correspon una sentència $\sigma_\gamma \in \text{Pred}(\mathbf{L}_{\text{ar}})$ que ◀ 17

$$\vdash_{\mathbf{T}} \neg\gamma^*(\mathbf{n}) \longleftrightarrow \sigma_\gamma.$$

Desfem els símbols predicatius i funcionals d'acord amb les seves definicions formals. Obtenim una sentència $\neg\gamma(\mathbf{n})$ de $\text{Pred}(\mathbf{L}_{\text{ar}})$ que $\vdash_{\mathbf{T}} \neg\gamma(\mathbf{n}) \longleftrightarrow \neg\gamma^*(\mathbf{n})$. Per tant,

$$\vdash_{\mathbf{T}} \neg\gamma(\mathbf{n}) \longleftrightarrow \sigma_\gamma.$$

Però ara ambdues sentències pertanyen al llenguatge $\mathbf{L}_{\text{ar}}$.
Per tant, si la teoria $\mathbf{T}$ satisfà la hipòtesi auxiliar, tenim, dins la teoria $\mathbf{P}$:

$$\vdash_{\mathbf{P}} \neg\gamma(\mathbf{n}) \longleftrightarrow \sigma_\gamma.$$

Fem: $\mathtt{Teorema_P}(v_1) := \exists v_2 \mathbf{Dem_P}(v_2, v_1)$.

En definitiva, amb força tècnica i un ús acurat del formalisme, es poden demostrar els teoremes formals 1), 2), 3), 1′), 4) i 5). ◀ 20

Per acabar, cal que indiquem una sentència $\mathtt{Consist_P}$. Per exemple,

$$\mathtt{Consist_P} := \neg\forall v_1 \Big(\mathbf{Form_P}(v_1) \longrightarrow \mathtt{Teorema_P}(v_1)\Big).$$

6.– El primer problema de Hilbert. Fa referència també a la possibilitat de demostrar, o **no**, una sentència dins una teoria formal.

1938: Gödel fa la primera aportació. Dona un model $\mathbb{L}$ en el qual un conjunt té **molts pocs** subconjunts perquè en realitat només agafa els que s'obtenen per mitjà de fórmules del llenguatge.

En cada pas del nivell de l'estructura $\mathbb{L}$,

$$L_{\alpha+1} := \mathrm{Def}\Big(L_\alpha \cup \{L_\alpha\}\Big).$$

$$L_\lambda := \bigcup L_\alpha, \lambda \in \mathbb{L}\text{ím}.$$

Hi ha pocs conjunts en cada L_α:

1) $\mathrm{card}(L_\alpha) = \mathrm{card}(\alpha)$;
2) Si $x \in L_\kappa, \kappa \in \mathbb{C}\mathrm{ard}$, aleshores $\mathcal{P}(x) \subseteq L_{\kappa^+}$.

$\mathbb{L}$ és l'univers dels conjunts definibles o constructibles.

A l'univers $\mathbb{L}$ valen l'axioma de l'elecció ($\mathbf{AC}$) i la hipòtesi general del continu ($\mathbf{HGC}$).

Si admetem l'**axioma de constructibilidad**: $\mathbb{V} = \mathbb{L}$,

óbviament, a l'univers $\mathbb{V}$ de **tots** els conjunts, valen el $\mathbf{AC}$ i la $\mathbf{HGC}$.

Dues observacions.

a) Gödel usa nou funcions per introduir els conjunts construïbles, en analogia al que havia fet per introduir les funcions recursives. Això fa que saigui fàcil, establir que $\mathbb{L}$ satisfà l'$\mathbf{AC}$.

b) Si tenim l'axioma de les parts perquè necessitem el d'especificació? Els conjunts produïts per un conjunt donat X i una fórmula $\alpha(v_1)$ no és un subconjunt de X i, per tant, no pertany a $P(X)$?

És a dir, $Y = \{x \in X : \alpha(x)\} \subseteq X$?

1963/64: Paul R. Cohen força l'existència de conjunts —d'alguna manera són conjunts imaginaris.

Per aconseguir-ho, necessita una mena de models $\mathbb{M}[G]$, transitius però **no** són interns ja que la relació de pertinença **no** és la induïda per $\in$

▶ Per fer-ho, li cal un conjunt $G \notin \mathbb{M}$ que li permiti generar un model $\mathbb{M}[G]$ en el qual $\mathbb{O}\mathrm{rd}$ sigui la classe dels ordinals del univers.

La tècnica del forcing és molt sofisticada i la comprensió intuïtiva és pràcticament nul·la.

Tanmateix, atès que podem afegir conjunts en quantitat arbitrària, no ens ha extranyar que s'aconsegueixi que, en aquest model, $\mathcal{P}(\omega)$ —és a dir, $2^{\aleph_0}$— sigui estrictament més gran que $\aleph_1$; per exemple, $\aleph_2$.

Objetiu. Allò que realment interessa és saber perquè podem **veure** $\mathcal{P}(X)$ de manera diferent segons en quin model el mirem, malgrat que X sigui un element del model.

1938: El leitmotiv el trobem en el treball de Gödel. Són les fórmules i els termes **absoluts**.

Definició 6.1. Sea $\mathbb{M}$ una classe transitiva. Una fórmula $\varphi(v_1, \ldots, v_k) \in \mathrm{Pred}(\mathbf{L}_{\mathrm{con}})$. $\varphi(v_1, \ldots, v_k)$ és $\mathbb{M}$-absoluta si, i només si, per a tota k-pla $x_1, \ldots, x_k \in \mathbb{M}$,

$$\mathbb{M} \models \varphi(x_1, \ldots, x_k) \text{ si, i només si, } [\vdash_{\mathbf{ZF}}] \varphi(x_1, \ldots, x_k).$$

Un terme t és $\mathbb{M}$-absolut si, i només si, la fórmula $z = t$ ho és.

- Diem simplement que són absoluts quan ho són per a tota classe transitiva $\mathbb{M}$.

La major part de las fórmules i termes que es manegen en la formulació bàsica de la teoria de conjunts ($\mathbf{ZF}$) són absoluts.

Això fa que l'estudi de l'absolutesa no sigui, en absolut, irrellevant.

1961: Dana Scott demostra que hi ha teories axiomàtiques de conjunts en les quals $\left(\mathcal{P}(\omega)\right)^{\mathbb{L}} \subsetneq \mathcal{P}(\omega)$.

Teorema de Scott. Si hi ha un cardinal mesurable, aleshores $\mathbb{V} \neq \mathbb{L}$.

En conseqüència, $\left(\mathcal{P}(\omega)\right)^{\mathbb{L}} \neq \mathcal{P}(\omega)$.

- De fet, $U = \left\{\alpha \in \kappa : \mu(\alpha) = 1\right\} \notin \mathbb{L}$.

Definició 6.3. Un cardinal κ és mesurable si, i només si, existeix un ultrafiltre sobre κ, U, no principal, κ-complet.

En definitiva, l'operador $\mathcal{P}(X)$ **no** és absolut.

1964: Frederick Robowtton va establir que, en certes condicions, $\aleph_1^{\mathbb{L}}$, considerat a $\mathbb{L}$, és numerable.

Teorema de Rowbottom. Si existeix un cardinal mesurable, $\aleph_1^{\mathbb{L}}$ és numerable.

- Aquest teorema **no** és, en absolut, elemental.

1965: Azriel Lévy, en un treball realment notable sobre la naturalesa formal de les fórmules utilitzades en la teoria de conjunts ($\mathbf{ZF}$ o $\mathbf{ZFC}$), introdueix la jerarquia de Lévy:

Definició 6.2. (**La jerarquia de Lévy**)

(a) Una fórmula φ está fitada si, i només si, tots els seus quantificadors (si n'hi ha) són de la forma $\forall x \in y, \exists x \in y$.

(b) Introduïm la classificació següent:

1) $\varphi \in \Sigma_0 = \Pi_0$ si, i només si, φ está fitada.
2) $\varphi \in \Sigma_{n+1}$ si, i només si, $\varphi := \exists x\, \psi(x)$, en què $\psi(x) \in \Pi_n$.
3) $\varphi \in \Pi_{n+1}$ si, i només si, $\varphi := \forall x\, \psi(x)$, en què $\psi(x) \in \Sigma_n$.

I fem $\Delta_n = \Sigma_n \cap \Pi_n$.

▶ En una teoría de conjunts $\mathbf{T} \subseteq \mathrm{Pred}(\mathbf{L}_{\mathrm{con}})$, un fórmula $\varphi \in \mathrm{Pred}(\mathbf{L}_{\mathrm{con}})$ és Σ_n, Π_n si, i només si, existeix una fórmula $\varphi^* \in \Sigma_n$ (respectivament $\varphi^* \in \Pi_n$) i $\vdash_{\mathbf{T}} \varphi \longleftrightarrow \varphi^*$.

Com en el cas de las fórmules absolutes, la major part de les fórmules bàsiques de la teoria de conjunts són Δ_0, Σ_1, Π_1 i, fins i tot, Δ_1.

Això és el que fa que sigui interessant estudiar-les.

Proposició 6.1. Totes les fórmules Δ_0 són absolutes.

- És una conseqüència elemental de les definicions.

  Totes les fórmules Δ_1 són absolutes.

- Això és així perquè les fórmules Σ_1 són absolutes cap amunt (del model a l'univers), i les Π_1, absolutes cap avall (de l'univers al model).

Hi ha un teorema anàleg al de Shoenfield per a les sentències existencials de $\mathbf{P}$ per a les de $\mathbf{ZF}$.

Teorema de Lévy-Shoenfield. Sigui φ una Σ_1-fórmual de $\mathrm{Pred}(\mathbf{L}_{\mathrm{con}})$. Aleshores

$$\vdash_{\mathbf{ZF}} \varphi \longleftrightarrow \varphi^{\mathbb{L}}.$$

Així doncs, atès que tota fórmula de Σ_1 és $\mathbb{L}$-absoluta, resulta que la validesa en $\mathbb{L}$ implica que sigui un teorema de $\mathbf{ZF}$.

- Els teoremes de la teoria de conjunts són tècnicament delicats.

Corol·lari 6.4. La sentència $\sigma_{\mathbf{HC}} := \aleph_1 \sim P(\aleph_0)$ **no** és Σ_1 atès que, segons els resultats de Cohen, $\not\vdash_{\mathbf{ZF}} \sigma_{\mathbf{HC}}$.

- Ara bé, encara **no** sabem si $P(x)$ és Σ_1.

- El teorema de Lévy permet establir-ho directament, però calen alguns conceptes previs:

Definició 6.4. (a) Donat un conjunt X, la clausura transitiva de X, $\mathrm{CT}(X)$ és el mínim conjunt transitiu que conté X.

(b) Per a cada $\kappa \in \mathbb{C}\mathrm{ard} - \omega$, $H(\kappa)$ és el conjunt dels conjunts que hereten el cardinal

$$H(\kappa) = \Big\{x : \mathrm{card}\Big(\mathrm{CT}(x)\Big) < \kappa\Big\}.$$

Teorema de Lévy (AC). Si $\varphi(v, v_1, \ldots, v_k)$ és Σ_1, $\mathrm{L}\Big(\varphi(v, v_1, \ldots, v_k)\Big) = \{v, v_1, \ldots, v_k\}$ i $\kappa > \omega$,

$$\forall x_1 \cdots \forall x_k \in H(\kappa)\Big(\exists x\, \varphi(x, x_1, \ldots, x_k) \longrightarrow \exists x \in H(\kappa)\, \varphi(x, x_1, \ldots, x_k)\Big).$$

- De fet, si $x_1, \ldots, x_k \in H(\kappa)$, $\vdash_{\mathbf{ZF}} \exists x \varphi(x, x_1, \ldots, x_k)$ implica $\models_{H(\kappa)} \varphi(x, x_1, \ldots, x_k)$.
  Vol tècnica: cal el principi de reflexió i el colapse de Mostowski.

Corol·lari (AC). (a) Si $t := t(v_1, \ldots, v_k)$ és un terme de Σ_1 i $x_1, \ldots, x_k \in H(\kappa)$, $t(x_1, , x_n) \in H(\kappa)$.

- Es inmediat a partir de les definicions.

(b) $\mathcal{P}(X)$ **no** és Σ_1.

- $\omega \in H(\aleph_1)$ i $\mathcal{P}(\omega) \notin H(\aleph_1)$.

L'operador $\mathcal{P}(X)$ **no** és absolut perquè **no** és Σ_1.

- És Π_1, però no és Δ_1.

▶ Aquests conjunts permeten establir una demostració relativament senzilla de la consistència relativa de la **HGC** perquè els L_κ i els $H(\kappa)$ estan relacionats.

Teorema de Gödel $(\mathbf{AC})$. Sigui $\kappa \in \mathbb{C}\mathrm{ard}$. Aleshores,

a) $\forall x\Big(x \in H(\kappa) \wedge x \in \mathbb{L} \longrightarrow x \in L_\kappa\Big)$.

b) $\forall x\Big(x \in L_\kappa \longrightarrow x \in H(\kappa)\Big)$.

▶ Hem d'establir que $\mathcal{P}(\kappa) \subseteq L_{\kappa^+}$.
Ara bé, si $x \subseteq \kappa$, $x \in H(\kappa^+)$. Si, a més, $x \in \mathbb{L}$, $x \in L_{\kappa^+}$. Per tant, $\mathcal{P}(\kappa) \in L_{\kappa^+}$.
En definitiva, $\kappa^+ \leq \mathrm{card}\Big(\mathcal{P}(\kappa)\Big) \leq \mathrm{card}\Big(L_{\kappa^+}\Big) \leq \kappa^+$.

Corol·lari $(\mathbf{AC})$. $\mathbf{ZFC} + \mathbb{L} = \mathbb{V} \vdash \mathbf{HGC}$.

▶ De fet, hem demostrat que $\vdash_{\mathbf{ZFC}} (\mathbf{HGC})^{\mathbb{L}}$. Però, $\vdash_{\mathbf{ZF}} (\mathbb{V} = \mathbb{L})^{\mathbb{L}}$. Per tant, $\vdash_{\mathbf{ZF}} (\mathbf{HGC})^{\mathbb{L}} \wedge (\mathbf{AC})^{\mathbb{L}}$.

7.– Conclusió. Hem exposat els detalls i hem vist que el concepte de recursividad enumerable, convenientement adaptat a cada problema, facilita la seva comprensió i els integra en un tot molt més coherent i clarificador.

Podem acabar amb les paraules amb què Hilbert acaba la conferència de 1900:

Em limitaré a fer notar fins a on és característic de la nostra Ciència el fet que cada progrés efectiu comporta el descobriment de mitjans auxiliars més rigorosos i més simples que, alhora que faciliten la comprensió de les teories anteriors i condueixen a la desaparició dels desenvolupaments precedents inútils, permeten orientar-nos en totes les branques de les Matemàtiques molt més fàcilment que en qualsevol altre Ciència.

El caràcter unitari de la Matemàtica en constitueix l'essència. En efecte, les Matemàtiques són el fonament de totes les ciències naturals exactes. Per tal que, en el segle que s'inicia, puguin complir totalment el seu elevat objectiu hauran de ser cultivades por mestres genials i per nombrosos joves inflamats per un noble zel.

8.– Uns altres problemes lligats amb les relacions i funcions r.e.

—El teorema de Fermat.
—La conjectura de Goldbach.
—La hipòtesi de Riemann.
—Podem donar un polinomi que generi els nombres primers.
—Podem demostrar i un teorema d'incompletesa diofàntic.

1900: A la conferencia, Hilbert, de passada o entre els vint-i-tres problemes, n'esmenta d'altres que podem relacionar amb el caràcter recursivament enumerable o diofàntic de certes relacions.

8.1–**Teorema de Fermat**. Per a cada n, l'equació diofàntica

$$(X+1)^{n+3}+(Y+1)^{n+3}=(Z+1)^{n+3}$$

no té solucions enteres poisitives.

És una equació exponencial diofàntica i per tant diofàntica. O sigui:

L'equació $(X+1)^{n+3}+(Y+1)^{n+3}=(Z+1)^{n+3}$ no té solucions enteres positives si, i només si, existeix una equación polinòmica $P(n,X,Y,Z,X_1,\ldots,X_k)=0$ sense solucions positives.

8.2– **Conjectura de Goldbach**. Tot nombre parell $2a+4$ és la suma de dos nombres primers senars.

Formalment, $\forall a \exists p_1 \exists p_2 \big((2a+4 = p_1 + p_2) \wedge Primer(p_1) \wedge Primer(p_2)\big)$.

Recordem que la propietat numèrica $Primer(p)$ és diofàntica.

La conjectura de Goldbach proporciona una família paramètrica d'equacions diofàntiques de paràmetre a. La negació, en canvi, estableix que

Conjectura negativa de Goldbach. Diu:

$$\forall z < a \, \exists x \, \exists y \, \big(z+2 = (x+2)(y+2) \vee (2a+4-z) = (x+2)(y+2)\big),$$

que és una equació diofàntica $D(x_0, \ldots, x_k) = 0$ que té solucions.

- La conjectura de Goldbach estableix, doncs, que la equació diofàntica anterior **sense** soluciones.

8.3– **Hipótesis de Riemann**. *Els únics zeros, no trivials, de la funció $\zeta(z)$ de Riemann, en els complexos, obtinguda per extensió analítica de $\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$, són a la recta $Re(z) = \frac{1}{2}$.*

Segons les aportacions de Davis, Matijasevicz i Robinson, si usem la función ψ de Chebychev: $\psi(n) = \ln\big(\text{mcm}(1, 2, \ldots, n)\big)$, tenim que

La Hipòtesi de Riemann és equivalent a $\psi(n) = n + O\big(\sqrt{n}\ln^2(n)\big)$.

▶ Per a $n \geq 600$, l'error s'expressa en la forma: $\big|\psi(n) - n\big| < \sqrt{n}\ln^2(n)$.

Per a evitar el logaritme ln, introduïm la relación següent:

$$\text{logexp}(a, b) := \exists x \left(x > b + 1 \wedge \left(1 + \frac{1}{x}\right)^{xb} \leq a + 1 < 4 \left(1 + \frac{1}{x}\right)^{xb} \right),$$

de propietats relativament elementals.

La negació de la Hipòtesi de Riemann equival a l'existència dels nombres k, ℓ, m i n:

1) $n \geq 600, m > 0$;
2) $\forall y < n\big((y + 1)|m\big)$ [que proporciona un comú múltiple de $1, 2, \ldots, n$];
3) $\forall y < m\big(y = 0 \vee \exists x < n\big((x + 1) \not| (y)\big)\big)$ [que dona el mcm de $1, 2, \ldots, n$];

i les tres que provenen de la substitució de ln per logexp:

4) $\text{logexp}(m - 1, \ell)$; 5) $\text{logexp}(n - 1, k)$; 6) $(\ell - n)^2 > 4n^2k^2$.

Totes són diofàntiques.

La Hipòtesi de Riemann equival a la irresolubilitat d'una equació diofàntica.

▶ La demostració és senzilla. El més delicat és veure que la Hipòtesi de Riemann es pot espressar en termes de la funció ψ.

8.4– **El conjunt dels nombres primers**. 1960: Hilary Putnam estableix el teorema:

Teorema de Putnam. Tot conjunt diofàntic D és la imatge positiva d'un polinomi.

$$m \in D \text{ si, i només si, } \exists x_1 \cdots \exists x_k \Big(P(x_1, \ldots, x_k) = m \Big).$$

- La implicació $\leftarrow$ és evident ja que $P(x_1, \ldots, x_k) = m$ és una relació recursiva.

  Per a la implicació $\rightarrow$, atès que D és diofàntic, hi ha un polinomi $Q(X_0, X_1, \ldots, X_k)$ que

  $$m \in D \quad \text{si, i només si,} \quad m > 0 \wedge \exists x_1 \cdots \exists x_k \Big(Q(m, x_1, \ldots, x_k) = 0 \Big).$$

  Considerem el polinomi $P(X_0, X_1, \ldots, X_k) = X_0 \Big(1 - Q^2(X_0, X_1, \ldots, X_k) \Big)$. És el que busquem.

$\leftarrow$ Suposem que $m \in D$. Aleshores existeixen $x_1, \ldots, x_k \in \mathbb{N}$ per als quals $Q(m, x_1, \ldots, x_k) = 0$. Per tant, $P(m, x_1, \ldots, x_k) = m$.

$\rightarrow$ Si $m = P(n, x_1, \ldots, x_k) > 0$, aleshores, per la definició del polinomi P, tenim que $m > 0$ i $1 - Q^2(n, x_1, \ldots, x_k) > 0$.

Per tant, $Q(n, x_1, \ldots, x_k) = 0$, ja que, en cas contrari, $1 - Q^2(n, x_1, \ldots, x_k) \leq 0$.

$Primer(n)$ és diofàntic. És la imatge positiva d'un polinomi. Quin?

1976: J. Jones, D. Sato, H. Wada i D. Wiens van donar-lo. Té 26 variables i grau 25. Es el següent:

$$
\begin{aligned}
(k+2)\Big\{ & 1-\big(wz+h+j-q\big)^2 \\
& -\big((gk+2g+k+1)(h+j)+h-z\big)^2 \\
& -(2n+p+q+z-e)^2 \\
& -\big(16(k+1)^3(k+2)(n+1)^2+1-f^2\big)^2 \\
& -\big(e^3(e+2)(a+1)^2+1-o^2\big)^2 \\
& -\big((a^2-1)y^2+1-x^2\big)^2 \\
& -\big(16r^2y^4(a^2-1)+1-u^2\big)^2-\big(\big((a+u^2(u^2-a)\big)^2-1\big)(n+4dy)^2+1-(x+cu)^2\big)^2 \\
& -(n+\ell+v-y)^2 \\
& -\big((a^2-1)\ell^2+1-m^2\big)^2 \\
& -(ai+k+1-\ell-i)^2 \\
& -\big(p+\ell(a-n-1)+b(2an+2a-n^2-2n-2)-m\big)^2 \\
& -\big(q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x\big)^2 \\
& -\big(z+p\ell(a-p)+\ell(2ap+2a-p^2-1)-pm\big)^2\Big\}.
\end{aligned}
$$

▶ Es la traducció pacient dels termes que hi ha a la definició diofàntica del conjunt dels nombres primers.

8.5–Podem establir el teorema de Gödel en termes diofàntics:

8.5– **Teorema diofàntic de incompletesa.** Sigui $\mathbf{T}$ una teoria consistent diofàntica; és a dir, el conjunt $AX_{\mathbf{T}}(n)$ és diofàntic. Aleshores existeix una equació diofàntica $P(X_1,\ldots,X_m)=0$ que **no** admet cap solució, però **no** és possible provar-ho a $\mathbf{T}$. Es a dir,

$$\not\vdash_{\mathbf{T}} \neg\exists x_1\cdots\exists x_m\Big(P(X_1,\ldots,X_m)=0\Big).$$

- El conjunt $E=\Big\{n\in\mathbb{N}: n=\text{god}(P) \text{ i } \not\vdash_{\mathbf{T}}\exists v_1\cdots\exists v_m\Big(P(v_1,\ldots,v_m)=0\Big)\Big\}$ és r.e.

perquè $Dem_{\mathbf{T}}(m,n)$ ho és.

Existeix $Q(X_0,X_1,\ldots,X_r)$ que caracteritza el conjunt E.

És a dir, $n\in E$ si, i només si, $Q(n,X_1,\ldots,X_r)=0$ és resoluble en $\mathbb{N}$.

Si $k=g\Big(Q(X_0,X_1,\ldots,X_r)\Big)$, aleshores

$k\in E$ si, i només si, $\exists x_1\cdots\exists x_r Q(k,x_1,\ldots,x_r)=0$. D'on: $\vdash_{\mathbf{T}}\exists v_1\cdots\exists v_r Q(\mathbf{k},v_1,\ldots,v_r)=0$.

$k\in E$ si, i només si, $\vdash_{\mathbf{T}}\neg\exists v_1\cdots\exists v_r Q(\mathbf{k},v_1,\ldots,v_r)=0$.

La primera condició es pot demostrar si la teoría és consistent $\mathbf{T}$. Contradicció.

Bibliografia

Davis, Martin
1973 «Hilbert's Problem Is Unsolvable». *The American Mathematica Montly*, **80**, 233–269.
2000 *The Universal Computer*. W.W. Norton & company, cop. Nova York. Traducció castellana de R. García, *La computadora universal*. Debate. Madrid, 2002.

Davis, Martin; Matijasevicz, Yuri; Robinson, Julia
1976 Hilbert's Tenth Problem. Diophantine equations: positive aspects of a negative solution, en *Mathematical Developments Arising from Hilbert Problems*, volumen 28 de *Proceedings of Symposia in Pure Mathematics*, 323–378. Providence. Rhode Island. American Mathematical Society.

Drake, Frank R.
1974 *Set Theory. An Introduction to Large Cardinals*. North-Holland Publishing. Amsterdam.

Epstein, Richard L.; Carnelli, Walter A.
1989 *Computability. Computable Functions, Logic, and the Foundations of Mathematics*. Wadsworth & Brooks/Cole. Pacific Grove. Califòrnia.

Gray, Jeremy
2000 *The Hilbert challenge*. Oxford University Press. Oxford.

Hilbert, David
1900 «Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker-Congress zu Paris 1900». *Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen*, 253–297.

Jech, Thomas J.
1978 *Set Theory*. Academic Press. Nueva York. Reeditat per Springer-Verlag. Berlín, 1997.

Moore, Gregory H.
1980 Beyond First Order Logic: The Historical Interplkay between Mathe-matical Logic and Axiomatic Set Theory. *History and Philosophy of Logic*, **1**, 95–137.
1988 «A house divided against itself: The emergence of fisrt-order logic as the basis for Mathematics», a Phillips, E. R. [1987], 98–136.

Matijasewicz, Yuri
1993 *Hilbert's Tenth Problem*. MIT Press. Cambridge.

Phillips, Esther R.
1987 *Studies in the history of mathematics*. Mathematical Association of America. [Washington, D.C.]

Pla, Josep
1991 *Lliçons de Lògica. Primera i Segona parts*. PPU. Barcelona.

Rosselló, Joan
2003 *Lògica i fonaments 1850–1920. Un estudi comparatiu de les contribucions del corrent algèbric i logicista a la lògica contemporània*. Tesi doctoral. Universitat de Barcelona. Barcelona.

Shoenfield, Joseph R.
1967 *Mathematical Logic*. Addison-Wesley. Boston.