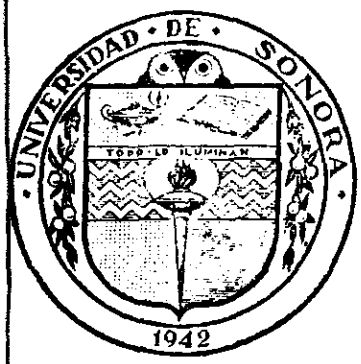

EL SABER DE MIS HIJOS
HARA MI GRANDEZA

UNIVERSIDAD DE SONORA

ESCUELA DE ALTOS ESTUDIOS

Decidibilidad, Resolubilidad y Algoritmia en Matemáticas

T E S I S

Que para obtener el título de:

LICENCIADO EN MATEMATICAS

p r e s e n t a :

Micaela Guadalupe Avila Godoy

Hermosillo, Son. 1979

Al compañero de mi vida,
compañero de carrera,
por su estímulo constante a mi formación y superación profesional.

Al pequeño Agustín
con todo mi amor.

A mi padre,
todo un ejemplo.

A mi madre,
imagen misma del cariño
y la ternura.

Con agradecimiento al profesor Enrique Valle Flores, por su invaluable y gran ayuda durante mi carrera y en la elaboración de esta tesis.

I N D I C E

P R Ó L O G O

Lo que se pretende es este trabajo es ilustrar con - ejemplos no triviales las naciones de Decidibilidad, Resolubilidad y Algoritmia en Matemáticas.

Los ejemplos que aquí se exponen, se encuadran fundamentalmente dentro de dos grandes escuelas del pensamiento matemático: el formalismo y el intuicionismo, y algunas de las características de éstas se muestran, pues, a través de estos ejemplos. Ellos son: El Décimo Problema de Hilbert, El Problema de la Mortalidad de Conjuntos de Matrices sobre los Complejos y el Concepto de Constructibilidad de los Números Reales.

Tanto por el nivel y objetivos de este trabajo, como por las concepciones que la autora tiene al respecto, no- se encuentran en él, profundidad ni extensión en cuanto a las polémicas estrictamente filosóficas que estos conceptos han suscitado históricamente. Son muchas las ocasiones en que afortunadamente la práctica audaz y creativa - de las grandes mentes matemáticas han demostrado que detenerse ante los titubeos "filosóficos" sería renunciar al - desarrollo de las Matemáticas.

INTRODUCCIÓN

La construcción de las primeras geometrías no euclidianas (la Geometría Riemaniana y la Geometría Hiperbólica-Plana) por Riemann, Lobatschevsky, Gauss y Bolyai a principios del siglo pasado constituye el primer paso hacia el método axiomático moderno. El método axiomático deductivo* como era concebido por los griegos- y cuya mejor exposición se encuentra en los Elementos de Euclides- suponía que las proposiciones de la Matemática- en particular de la Geometría- eran expresión de propiedades de objetos reales, (así, pues, las demostraciones se apoyaban frecuentemente de una forma implícita en las naciones intuitivas que sobre estos objetos se tenía). El descubrimiento de Rieman, Gauss, Bolyai y Lobatschevsky viene a poner fin a los infructuosos intentos efectuados durante mucho tiempo por deducir el quinto postulado de Euclides a partir de los primeros cuatro; sus geometrías se obtienen como resultado de sustituir ese postulado por ciertas formas de su negación y obtener alternativas a la geometría euclideana, igualmente válidas desde el punto de vista matemático y aun desde el punto de vista físico. De acuerdo con la concepción clásica de una teoría Matemática, se suscitaba la cuestión de la "existencia" de estas geome

*Existencial.

trías, es decir, de la existencia de un sistema de objetos reales de nuestra institución, cuya "descripción" correspondiera a estas geometrías. Klein, Beltrami y Poincaré con sus modelos euclideos de estas geometrías no-euclideanas dan una respuesta a esta cuestión. Quedaba claro entonces que los axiomas y las proposiciones derivadas de ellos no constituían necesariamente la "descripción de un sistema de objetos reales determinados, sino que podían constituír las propiedades comunes de varios de tales sistemas diferentes, o sea que podían existir diferentes "interpretaciones" o "modelos" de una teoría matemática dada. Todo este desarrollo se refina y cristaliza en las "Grundlagen der Geometrie" de Hilbert y antes en la disertación inaugural de B. Riemann, en las teorías matemáticas las nociones primeras no son de una naturaleza específica, no tienen significación en si mismas, interesan nada más las relaciones entre ellas, establecidos en los axiomas, relaciones cuya significación tampoco importa. En este contexto, la "existencia" de una teoría matemática (sistema de axiomas, reglas de formación, reglas de transformación) se establece comprobando su no-contradictoriedad (Hilbert lo planteaba en el Segundo Congreso Internacional de 1900) es decir, que no pueden demostrarse en esa teoría, tanto alguna proposición (P) como su negación (no P). Clásicamente la no-contradictoriedad de un concepto únicamente garanti-

zaba su posibilidad. El problema de saber si el Quinto postulado de Euclides era decidible en el sistema de los otros cuatro axiomas de Euclides, i.e., si podía deducirse de ellos, se planteaba entonces en estos términos, como el problema de saber si las geometrías no-euclideanas resultaban contradictorias o no-contradictorias.

Tomando en cuenta los resultados que mencionamos de Riemann, Klein y Beltrani, la creación de la Geometría Analítica de Descartes (que da un "modelo geométrico" del análisis— del sistema de los números reales— y viceversa) y la "aritmetización del análisis" llevada a cabo por Weierstrass, Dedekind, Meray, y Cantor (que nos da una construcción de los números reales a partir de los naturales* reduciendo sus propiedades a la de estos últimos), la no contradicción de la aritmética arrojaría la no contradicción del análisis y de las geometrías euclidianas y no euclideanas. De ahí la enorme importancia del problema de la consistencía de la aritmética, el segundo de los problemas planteados por Hilbert, en su fomosa conferencia en el Congreso Internacional de 1900. Con más precisión: considerando a la aritmética como un sistema formalizado, i.e., formada por agrupaciones de signos sin significado y una serie de reglas que rigen la formación y

*El Sistema Axiomatizado de los Números Naturales dado por Dedekind y Peano a finales del siglo pasado.

encadenamiento de estas agrupaciones, no se podrá obtener nunca una proposición (agrupación de signos) mediante el uso de tales reglas de tal manera que también su negación pueda obtenerse.

Por otra parte el requisito de independencia de los axiomas de un sistema, es decir, que cada axioma sea una proposicioón no decidible en el sistema de axiomas reducido correspondiente, esto es, que ni el axioma ni su negación puede ser derivados de los axiomas restantes, es - equivalente al requisito de consistencia del sistema inicial y del sistema que resulta substituyendo en este el - axioma en cuestión por su negación. Surge así de una manera natural la pregunta ¿existe alguna proposición "formulable" en la teoría (que satisfaga las reglas de formación) tal que ni ella ni su negación puedan deducirse del sistema de axiomas de la aritmética; o sea, en un sentido también muy natural ¿es completa la aritmética?.

Hilbert propone un ambicioso programa en donde la - pregunta surgida en la exposición anterior- acerca de la Independencia, Consistencia y Completez de la aritmética- sea planteada al menos para toda la matemática clásica y- la teoría de conjuntos, previa su formalización. El sistema formal pasa a ser así objeto de estudio (para probar di

rectamente la consistencia de una teoría, debemos probar una proposición acerca de la teoría misma– y no dentro de ella– específicamente acerca de todas las posibles secuencias de agrupaciones (pruebas) de la teoría que fue llamado por Hilbert la Metatoría del Sistema Formal inicial.- Por lo que se refiere a la aritmética, los trabajos de - Gödel demostraron la imposibilidad de llevar a cabo los - objetivos del programa de Hilbert. Gödel probó que no es posible demostrar por métodos matemáticos la consistencia de la aritmética y que esta es esencialmente incompleta,- es decir, que el cualquier sistema formal que contenga a la aritmética siempre habrá proposiciones indecidibles. - Los trabajos de Gödel establecen la posibilidad de que - conjeturas de la aritmética y del análisis que han resistido los esfuerzos de grandes matemáticos– conjeturas de Fermant, Goldbach y Riemann entre ellas– resulten proposiciones indecidibles. En los diversos sistemas de axiomas que se han elaborado para la teoría de conjuntos han surgido numerosas proposiciones indecidibles, quizá la más - famosa de ellas es la hipótesis del continuo, cuyo caracter indecidible a partir de los axiomas de Zermelo– Fraenkel y el axioma de elección fue aprobado por Cohen y - Gödel.

Como ya habíamos explicado en la fundamentación axio-

mática de las matemáticas una proposición es verdadera -con solo no ser contradictoria. En las proposiciones de existencia, por ejemplo, basta con probar que esta no contradice los axiomas del sistema. La escuela intuicionista o constructiva rechaza este punto de vista y solo acepta como válida la demostración que prescribe un procedimiento (de un número finito de pasos) esto es un algoritmo- para la construcción del objeto.

En los capítulos I y II de este trabajo se discute el concepto de algoritmos y su relación con la decidibilidad a travez de dos problemas de existencia de algoritmos y en el capiítulo III de da un enfoque constructivista del sistema de los números reales, donde el concepto de decidibilidad juega un papel primordial.

CAPITULO I

EL DECIMO PROBLEMA DE HILBERT

1. CONJUNTOS Y ECUACIONES DIOFANTINAS

Definición 1.1. Una ecuación es llamada diofantina si sus coeficientes y sus exponentes son enteros.

Por ejemplo:

$$5x^{18} - 9xy^6uv^2 + 109\ z^3 - 6 = 0$$

Definición 1.2. Un conjunto S de n-adas ordenadas de enteros positivos es llamado diofantino si existe un polinomio $P(\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}, \ldots, \alpha_{n+m})$, donde $n+m \geq n$, con coeficientes enteros tal que una n-ada $(x_1, \ldots, x_n) \in S$ si y solo si

$$P(x_1, \ldots, x_n, \alpha_{n+1}, \ldots, \alpha_{n+m}) = 0$$

tiene solución en los enteros pisitivos.

Esto es:

$$S = \{(x_1, \ldots, x_n) : (\exists y_1, \ldots, y_m)\ [P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\}.$$

Note que P debe tener coeficientes negativos.

Los siguientes son ejemplos de conjuntos diofantinos:

i) Los números que no son potencia de dos

$$S = \{x : (\exists y, z)\ [x = y(2z + 1)]\}$$

El polinomio es: $P(x,y,z) = x - y(2z + 1)$

ii) Los números compuestos

$$S = \{x : (\exists y, z)\ [x = (y + 1)(z + 1)]\}$$

El polinomio es: $P(x,y,z) = x - (y + 1)(z + 1)$

iii) Los conjuntos:

$$\{(x, y) : x < y\} \quad y \quad \{(x,y) : x \leqslant y\}$$

Los polinomios son:

$$P(x,y,z) = y - x - z \quad y \quad P(x,y,z) = y - x - z + 1$$

respectivamente.

iv) $\{(x,y) : x\ y\}$

El polinomio es:

$$P(x,y,z) = x - yz$$

v) $\{(x,y,z) : x|y \quad y \quad x < z\}$

El polinomio es:

$$P(x,y,z,u,v) = (y - ux)^2 + (z - x - v)^2$$

Note que la técnica usada en v) es general. Para definir un conjunto Diofantino se puede usar un sistema simultáneo

$$P_1 = 0, \quad P_2 = 0, \ldots, P_k = 0$$

de ecuaciones polinomiales, ya que este puede ser reemplazado por la ecuación equivalente

$$P_1^2 + P_2^2 + \ldots + P_k^2 = 0$$

2. FUNCIONES DIOFANTINAS

<u>Definición 2.1</u>. Una función ϕ de n variables es llamada Diofantina si

$$\{(x_1,\ldots,x_n,y) : y = \phi(x_1,\ldots,x_n)\}$$

es diofantino.

Es decir, ϕ es Diofantina si su gráfica es un conjunto Diofantino.

Una función Dofantina muy importante está asociada con los números triangulares, es decir, los que son de la forma

$$T(n) = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

ya que $T(n)$ es creciente, para cada $z \in \mathbb{Z}^+$, existe un n único tal que

$$T(n) < z \leq T(n+1) = T(n) + n + 1$$

Por esto, z tiene una representación única

$$z = T(n) + y \quad \text{donde} \quad 1 \leq y \leq n + 1$$

o equivalente $z = T(x + y - 2) + y \quad , \quad x \geq 1$

Esta función

$$P(x,y) = T(x+y-2) + y$$

mapea el conjunto de pares ordenados de números naturales en los números naturales de acuerdo al siguiente diagrama:

		y				
	P(x,y)	1	2	3	4	5
	1	1	3	6	10	15
	2	2	5	9	14	
x	3	4	8	13		
	4	7	12			
	5	11				

Las dos funciones inversas L y R están univocamente determinadas para la ecuación

$$z = P(L(z), R(z))$$

Los primeros valores de L y R los cuales claramente indican el patrón general de sus sucesiones de valores están dados como sigue:

z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
L(z)	1	2	1	3	2	1	4	3	2	1	5	4	3	2	1
R(z)	1	1	2	1	2	3	1	2	3	4	1	2	3	4	5

Nótese que $P(x,y)$, $L(z)$ y $R(z)$ son funciones diofantinas ya que

$$z = P(x,y) \iff 2z = (x+y-2)(x+y-1) + 2y$$

$$x = L(z) \iff (\exists y)\,[2z=(x+y-2)(x+y-1) + 2y]$$

$$y = R(z) \iff (\exists x)\,[2z=(x+y-2)(x+y-1) + 2y]$$

Es claro que $P(x,y)$ es una a uno y sobre. También nótese que $L(z) \leq z$ y $R(z) \leq z$.

Lo anterior lo resumimos en el siguiente teorema:

Teorema 2.1. (Teorema de la Función Apareadora). Existen funciones diofantinas

$$P(x,y),\ L(z) \quad y \quad R(z)$$

tales que:

i) Para todas x, y, $L(P(x,y)) = x$

y $R(P(x,y)) = y$

ii) Para toda z, $P(L(z),R(z)) = z$, $L(z) \leq z$

y $R(z) \leq z$.

Definimos otra función diofantina muy importante - después de demostrar el Teorema Chino del Residuo establecido abajo:

Teorema 2.2. (Teorema Chino del Residuo). Sean $a_1, a_2, \ldots, a_N$ cualesquiera enteros positivos y sean $m_1, m_2, \ldots, m_N$ enteros positivos tales que

$$(m_i, m_j) = 1 \quad \text{si} \quad i \neq j.$$

Entonces, existe x tal que

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_N \mod m_N \end{aligned}$$

Esta solución es única, módulo $m = m_1 m_2 \ldots m_N$

Demostración. Sea $\tau_i = \frac{m}{m_i}$, $1 \leq i \leq N$ Entonces $(\tau_i, m_i) = 1$ pues los m_i son primos relativos - por pares. Por esto podemos determinar un m_i tal que

$$\tau_i \; m_i' \equiv 1 \mod m_i \quad 1 \leq i \leq N$$

Pero, entonces

$$x = \sum_{i=1}^{n} \tau_i \; m_i' a_i$$

es solución del sistema. Además, si x, y son soluciones del sistema, deben satisfacer

$$x - y \equiv 0 \mod m_i \quad 1 \leq i \leq N$$

y de aquí

$$x - y \equiv 0 \mod m \text{ , es decir}$$

$$x \equiv y \mod m$$

porque las m_i son primos relativos por pares.

Ahora, definamosla función $S(i,u)$ de la siguiente manera:

$$S(i,u) = \omega$$

donde ω es el único entero positivo para el cual

$$\omega \equiv L(u) \mod (1 + i\, R(u))$$

con

$$\omega \leqslant 1 + iR(u)$$

Teorema 2.3. (Teorema Diofantino de la Sucesión de Números). Existe una función Diofantina $S(i,u)$ tal que

1) $S(i,u) \leqslant u$.

2) Para cada sucesión $a_1 \ldots\ldots a_n$ existe u. tal que

$$S(i,u) = a_i \qquad 1 \leqslant i \leqslant n$$

Demostración. Primero vamos a demostrar que $S(i,u)$ es una función Dofantina. Para esto, lo que se pretende es ver que

$$\omega = S(i,u)$$

$$<=>$$

$$2u = (x+y-2)\ (x+y-1) + 2y$$

$$x = \omega + z(1+iy)$$

$$1+iy = \omega + v - 1$$

este sistema de ecuaciones tiene solución. Esto es claro porque la primera ecuación es equivalente a

$$x = L(u) \quad y \quad y = R(u)$$

Ahora,

$$S(i,u) = \omega \leqslant L(u) \leqslant u$$

Por último, sean $a_1,\ldots,a_n$ números dados. Escojemos y de tal manera que $y > a_i$ para $i = 1,\ldots,n$ y $1 \mid y,\ 2 \mid y,\ldots,n \mid y$.

Entonces los números $1 + y,\ 1 + 2y,\ldots,1 + ny$ son primos relativos por pares (supongamos que existe d tal que $d \mid 1+iy$ y $d \mid 1+jy$, $i < j$; entonces

$$d \mid [(1+iy) - (1+jy)]$$

es decir $d \mid j-i$ esto es, $d \leqslant n$; pero $d \leqslant n$ es imposible pues $d \mid y$ y d no dividiría a $1 + iy$. Aplicamos el Teorema Chino del Residuo para obtener un x tal que

$$\begin{aligned} x &\equiv a_1 \pmod{1 + y} \\ x &\equiv a_2 \pmod{1 + 2^y} \\ &\vdots \\ x &\equiv a_n \pmod{1 + ny} \end{aligned}$$

Sea $u = P(x,y)$ de modo que $x = L(u)$ y $y = R(u)$.

Entonces

$$a_i \equiv L(u) \mod 1 + i\, R(u) \qquad i = 1,\ldots,n$$

y

$$a_i < y = R(u) < 1 + i\ R(u).$$

Pero de aquí por definición,

$$S(i,u) = a_i .$$

Una familia muy famosa de ecuaciones Diofantinos - tiene la forma

$$x^n + y^n = z^n , \qquad n \text{ entero.}$$

Si $n = 2$, la ecuación es llamada el Teorema de Pitágoras y una solución es

$$x = 3 , \quad y = 4 , \quad z = 5.$$

Si $n \geq 3$, la ecuación es conocida como la ecuación Fermat. En el siglo 17 el matemático francés Pierre de Fermat pensó que había probado que estas ecuaciones no tienen soluciones enteras positivos. Al margen de su copia del libro de Diofanto escribió que había encontrado una - "prueba maravillosa" que desafortunadamente era muy extensa para escribrila en ese espacio. La prueba nunca ha sido

encontrada. El conocido Teorema de Fermat es probablemente el más viejo y más famoso problema no resuelto en Matemáticas. Estos ejemplos prueban que las ecuaciones Dofantinas son fáciles de escribir y difíciles de resolver.

3. FUNCIONES RECURSIVAS

Las Funciones recursivas son aquellas que pueden ser calculadas por máquinas computadoras o programas finitos teniendo cantidades de tiempo y memoria arbirariamente grandes a su disposición. Existen varias definiciones rigurosas de esta clase (todas ellas equivalentes). Una de las más sencillas es la siguiente:

Definición 3.1. Las funciones recursivas son aquellas obtenibles de las funciones iniciales:

$C(x) = 1$, $S(x) = x + 1$, $U_i^n(x_1,\ldots,x_n)=x_i$ $i\leq i\leq n$, y $S(i,u)$

iterativamente aplicando las tres operaciones: composición, recursión primitiva y minimización definidas como sigue:

Composición. Sean $\delta : \mathbb{N}^m \to \mathbb{N}$ y $g_i : \mathbb{N}^n \to \mathbb{N}$, $i=1,2,\ldots,m$.

Se obtiene una nueva función

$$h = \delta_0 \ G : \mathbb{N}^n \to \mathbb{N} \text{ donde } G = (g_1, \ldots, g_m)$$

tal que

$$h(x_1, \ldots, x_n) = (\delta_0 G)\ (x_1, \ldots, x_n)$$

$$= \delta(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$$

<u>Recursión Primitiva</u>. Sean $\delta : \mathbb{N}^n \to \mathbb{N}$ y

$$g : \mathbb{N}^{n+2} \to \mathbb{N}.$$

Se obtiene una nueva función

$$h = \delta_R g : \mathbb{N}^{n+1} \to \mathbb{N}$$

tal que

$$h(x_1, \ldots, x_n, 1) = \delta(x_1, \ldots, x_n)$$

$$h(x_1, x_2, \ldots, x_n, t+1) = g(t, h(x_1, \ldots, x_n, t), x_1, \ldots, x_n)$$

Cuando $n = 0$, δ es una constante y h se obtiene directamente de g.

<u>Minimización</u>. Sean $\delta, g : \mathbb{N}^{n+1} \to \mathbb{N}$ tales que para cada $(x_1, \ldots, x_n)$,

$$A = \{y : f(x_1,\ldots,x_n,y) = g(x_1,\ldots,x_n,y)\} \neq \phi \ .$$

Se obtiene una nueva función

$$h : \mathbb{N}^n \to \mathbb{N}$$

tal que

$$h(x_1,\ldots,x_n) = \min_y \ A$$

Los siguientes son ejemplos de funciones recursivas:

i) $h(x,y) = x + y$

Aplicando la Composición a $S(x) = x + 1$ y

$$U_2^3 \ (u,v,w) = v$$

obtengo una nueva función g, tal que

$$g(u,v,w) = S(U_2^3 \ (u,v,w)) = \ S(v) = v + 1 \ .$$

Aplicando la Recursión primitiva a

$$S(x) = x + 1 \quad y \quad g(u,v,w) = v + 1,$$

obtengo una nueva función h,

$$h(x,1) = S(x) = x + 1$$

$$h(x,t+1) = a(t,x+t,x) = (x+t) + 1 = x+(t+1)$$

ii) $\delta(x,y) = x \cdot y$

Aplicando la Recursión primitiva a

$g(u,v,w) = U_2^3(u,v,w) + U_3^3(u,v,w) = v+w$ y $U_1^1(x) = x \cdot 1$

obtengo una nueva función δ

$$\delta(x,1) = U_1^1(x) = x \cdot 1$$

$$\delta(x,t+1) = g(t,x \cdot t,x) = x \cdot t + x = x(t+1)$$

iii) Para cada k fijo $C_k(x) = k$ es recursiva, ya que $C_1(x)$ es una de las funciones iniciales y $C_{k+1}(x) = C_k(x) + C_1(x)$.

iv) Cualquier polinomio $P(x_1,\ldots,x_n)$ con coeficientes enteros positivos es recursiva ya que se puede expresar por un número finito de sumas y multiplicaciones de variables y $C(x)$; *i.e.*,

$$2x^2y + 3xz^3 + 5 = C_2(x) \cdot x \cdot x \cdot y + C_3(x) \cdot x \cdot z \cdot z \cdot z + C_5(x)$$

Así que, de *(i)*, *(ii)*, *(iii)* y la composición se tiene el resultado.

4. EL DECIMO PROBLEMA DE HILBERT

El Décimo Problema de Hilbert dice lo siguiente:

Dar un algoritmo mediante el cual cualquier ecuación diofantina pueda ser examinada para determinar si tiene soluciones enteras o no. Entendemos por algoritmo la preseripción exacta sobre el cumplimiento de cierto sistema de operaciones en un orden determinado para la resolución de todos los problemas de algún tipo dado. Dos peculiaridades de los algoritmos son las siguientes:

1º La precisión del algoritmo. Se exige que se pueda comunicar el método de cómputo a otra persona en forma de un número finito de indicaciones sobre cómo actuar en cada etapa del cálculo. En concordancia con estas indicaciones el cálculo no depende de la voluntariedad de la persona que lo hace y representa un proceso determinado que puede ser en cualquier momento repetido y cumplido con el mismo éxito por otra persona.

2º El amplio empleo del algoritmo. El algoritmo no soluciona solo un problema particular sino cier-

ta serie de problemas del mismo tipo.

Existe una profunda relación entre los algoritmos y las computadoras automáticas:

Cualquier proceso cuyas partes por separado se realizan consecutivamente en una computadora automática, puede ser descrito por un algoritmo.

Por otro lado, todos los algoritmos conocidos hasta ahora y también los que se pueden prever teniendo en cuenta el estado actual de la ciencia, en principio son realizables en computadoras automáticas.

El Décimo Problema de Hilbert es el décimo de la famosa lista que Hilbert presentó ante el Congreso Internacional de Matemáticos en 1900. El primer intento por probar que no existe algoritmo para el Décimo Problema de Hilbert fue hecho por Davis en su disertación doctoral en 1950. Lo que él probó es lo siguiente: Un entero positivo x pertenece a un conjunto listable* S si y solo si para algún valor entero positivo de z es posible encontrar una solución para cada una de las ecuaciones diofantinas substituyendo $k = 1$, después $k = 2$ y así sucesiva

*Un conjunto S de números naturales es listable si existe un algoritmo que determina si un número natural arbitrario pertenece a S. Listable es nuestro equivalente informal de recursivamente numerable.

mente hasta z en la ecuación

$$P(k, x, z, y_1, \ldots, y_n) = 0$$

Al mismo tiempo Julia Robinson empezó sus investigaciones sobre conjuntos que pueden ser definidos por ecuaciones diofantinas. Desarrolló varias técnicas ingeniosas para trabajar con ecuaciones cuyas soluciones crecieran exponencialmente.

En 1960, Davis, Robinson y Putman usando el trabajo de Robinson y el resultado de Davis, probaron el siguiente resultado: cualquier conjunto listable tiene una ecuación diofantina "extendida" correspondiente ("extendida" en el sentido de que las variables pueden ser exponentes; por ejemplo: $2^x + 3y^z = 0$).

También probaron: si se encontrara una ecuación diofantina cuyas soluciones crecieran exponencialmente sería posible describir cada conjunto listable por una ecuación diofantina.

Matiyasevich encontró una ecuación de este tipo, es decir, demostró: a cada conjunto listable le corresponde una ecuación diofantina. Con más precisión: Si S es

un conuunto listable entonces existe un correspondiente polinomio P con coeficientes enteros y variables

$$x,\ y_1,\ y_2,\ldots,y_n$$

que denotamos por

$$P_S(x,\ y_1,\ldots,y_n)$$

tal que $a \in S$ si y solo si

$$P_S(a,\ y_1,\ldots,y_n) = 0$$

tiene una solución.

Pero como Davis. Putman y Robinson ya habían encontrado un conjunto listable que no es computable*, el resultado de Matiyasevich llevó a que el Décimo Problema de Hilbert es irresoluble (esto lo exponemos en el parágrafo 6.).

* Un conjunto es computable si existe un algoritmo mediante el cual se determina si un número natural arbitrario n pertenece o no pertenece al conjunto.

5. EJEMPLOS DE CLASES DE ECUACIONES DIOFANTINAS PARA LOS CUALES EXISTEN ALGORITMOS QUE DETERMINAN SI TIENEN SOLUCIONES ENTERAS O NO

Sea la ecuación diofantina:

(1) $- - - - - - - ax + by = c$

Teorema 5.1. Sea $d = (a, b)$. La ecuación diofantina (1) tiene soluciones enteras si y solo si $d|c$.

Demostración. Ya que $d|a$, $d|b$ tenemos que $d|(ax + by)$ para todos los enteros x y y. Así que si

$$ax + by = c$$

entonces $d|c$. Por lo tanto (1) no tiene solución si $d \nmid c$.

Ahora supongamos que $d\ c$. Entonces existe un entero e tal que

$$c = de$$

También tenemos que existen enteros r y s tales que $ar + bs = d$

De aquí que

$$a(re) + b(se) = de = c$$

y (1) tiene una solución entera.

Sea la ecuación diofantina:

(2) $\quad - - - - - - - a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0$

Teorema 5.2. Si $\frac{p}{q}$ $(p,\ q \in \mathbb{Z}, (p,q) = 1)$ es solución de (2) entonces $q \mid a_0$ y $p \mid a_n$.

Demostración. Si $\frac{p}{q}$ es solución de (2) entonces

(3) $\quad - - - - - - - a_0 \frac{p^n}{q^n} + a_1 \frac{p^{n-1}}{q^{n-1}} + \ldots + a_{n-1} \frac{p}{q} + a_n = 0$

Multiplicando por q^{n-1}, tenemos

$$-a_0 \frac{p^n}{q} = a_1 p^{n-1} + \ldots + a_{n-1} p q^{n-2} + a_n q^{n-1}$$

y de aquí, $q \mid a_0$ Ahora multiplicando (3) por $\frac{q^n}{p}$, se tiene

$$a_0 p^{n-1} + a_1 p^{n-2} q + \ldots + a_{n-1} q^{n-1} = -a_n \frac{q^n}{p}$$

de donde $p \mid a_n$.

6. SOLUCION NEGATIVA DE MATIYASEVICH (EN LA VERSION DE DAVIS, PUTMAN Y ROBINSON) AL DECIMO PROBLEMA DE HILBERT.

Lo que se probará en esta sección es que no existe algoritmo para examinar un polinomio con coeficientes enteros que permita determinar si este tiene o no soluciones enteras positivas (Hilbert preguntó por las soluciones enteras arbitrarias). Pero de esto se seguirá que no existe algortimo para soluciones enteras. Porque entonces se podría examinar la existencia de soluciones enteras positivas $(x_1,\ldots,x_n)$ para la ecuación

$$P(x_1,\ldots,x_n) = 0$$

examinando la existencia de soluciones enteras

$$(p_1,\ q_1,\ r_1,\ s_1,\ldots,\ P_n,\ q_n,\ r_n,\ s_n)$$

para la ecuación

$$P(1+p_1^2+q_1^2+r_1^2+s_1^2,\ldots,\ 1+P_n^2+q_n^2+r_n^2+s_n^2) = 0 \quad .$$

Esto es porque (por el Teorema de Lagrange) todo entero no-negativo es la suma de cuatro cuadrados.

En el desarrollo de esta solución solo se tratará - con enteros positivos a menos que se establezca explícitamente lo contrario.

En esta exposición no se seguirá el desarrollo histórico del problema. El objetivo es hacer una exposición lo más suave y directa posible de los principales resultados.

6.1 24 LEMAS REFERENTES A LA ECUACION DE PELL.

Vamos a desarrollar los métodos que necesitaremos para probar que la función exponencial

$$h(n,k) = n^k$$

es Diofantina.

Sea la llamada ecuación de Pell.

$$(*) \qquad x^2 - dy^2 = 1 \ , \qquad x,\ y \geq 0$$

donde

$$d = a^2 - 1 \ , \qquad a > 1$$

Dos soluciones obvias de (*) son:

$$x = 1 \ , \ y = 0 \quad \text{y} \quad x = a \ , \ y = 1.$$

Lema 6.1.1. No existen enteros positivos, negativos

o el cero, los cuales satisfagan (*) y para los cuales

$$1 < x + y\sqrt{d} < a + \sqrt{d}$$

Demostración. Sean x, y los cuales satisfacen (*) y la desigualdad. Ya que

$$1 = (a + \sqrt{d})(a - \sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d})$$

la desigualdad implica (tomando recíproces)

$$-1 < -x + y\sqrt{d} < -a + \sqrt{d}$$

Sumando las desigualdades:

$$0 < 2y\sqrt{d} < 2\sqrt{d} \quad , \quad \text{es decir}$$

$$0 < y < 1 \qquad \text{(contradicción)}$$

Lema 6.1.2. Sean x, y y x', y' enteros positivos, negativos o el cero, los cuales satisfacen (*). Sea

$$x'' + y''\sqrt{d} = (x + y\sqrt{d})(x' + y'\sqrt{d})$$

Entonces x'' y y'' satisfacen*.

Demostración. Tomando conjugados, tenemos:

$$x'' - y''\sqrt{d} = (x - y\sqrt{d})(x' - y'\sqrt{d})$$

Multiplicando, tenemos

$$x''^2 - y''^2 d = (x^2 - y^2 d)(x'^2 - y'^2 d) = 1$$

Definición. $x_n(a)$, $y_n(a)$ son definidas para

$n \geq 0$, $a > 1$, así:

$$x_n(a) + y_n(a)\sqrt{d} = (a + \sqrt{d})^n$$

$x_n(a)$, $y_n(a)$

las escribiremos como x_n, y_n.

Lema 6.1.3. x_n, y_n satisfacen (*).

Demostración.

$$x_0 + y_0\sqrt{d} = (a + \sqrt{d})^0 = 1 = (1+0\sqrt{d})(1 + 0\sqrt{d})$$

Por el lema anterior x_0, y_0 satisfacen(*). Supongamos que x_n, y_n satisfacen(*); queremos demostrar que x_{n+1}, y_{n+1} son también soluciones de (*). Por definición,

$$x_{n+1} + y_{n+1}\sqrt{d} = (a+\sqrt{d})^{n+1}$$

$$= (a+\sqrt{d})^n (a+\sqrt{d})$$

$$= (x_n + y_n\sqrt{d})(a+\sqrt{d})$$

y por el lema anterior, x_{n+1}, y_{n+1} satisfacen (*).

Lema 6.1.4. Sean x, y soluciones no-negativas de (*). Entonces para algún n, $x = x_n$, $y = y_n$.

Demostración. Tenemos que $x + y\sqrt{d} \geq 1$. Por otro lado la sucesión

$$\{(a + \sqrt{d})^n\}$$

crece a infinito pues $a > 1$ y $\sqrt{d} > 0$. Para algún $n \geq 0$

$$(a + \sqrt{d})^n \leq x + y\sqrt{d} \leq (a + \sqrt{d})^{n+1}$$

Si se cumple la igualdad, ya tenemos

$$x + y\sqrt{d} = (a + \sqrt{d})^n = x_n + y_n\sqrt{d}$$

Ahora demostraremos que la desigualdad no puede cumplirse. Supongamos que se cumple. Tenemos

$$x_n + y_n\sqrt{d} < x + y\sqrt{d} < (x_n + y_n\sqrt{d})(a + \sqrt{d})$$

Multiplicando por $x_n - y_n\sqrt{d} > 0$

$$1 < (x + y\sqrt{d})(x_n - y_n\sqrt{d}) < a + \sqrt{d}$$

Demostración. $x_{m+n} + \sqrt{d}\, y_{m+n} = (a + \sqrt{d})^{m+n}$

$$= (a + \sqrt{d})^{m} (a + \sqrt{d})^{n}$$

$$= (x_m + \sqrt{d}\, y_m)(x_n + \sqrt{d}\, y_n)$$

$$= x_m x_n + d y_m y_n + (x_n y_m + x_m y_n)\sqrt{d}$$

De aquí tenemos

$$x_{m+n} = x_m x_n + d y_m y_n \quad y \quad y_{m+n} = x_n y_m + x_m y_n$$

Similarmente

$$(x_n + y_n\sqrt{d})(x_{m-n} + \sqrt{d}\, y_{m-n}) = (a+\sqrt{d})^{m-n} (x_n + y_n\sqrt{d})$$

$$= (a+\sqrt{d})^{m}$$

$$= x_m + y_m\sqrt{d}$$

Así

$$(x_{m-n} + \sqrt{d}\, y_{m-n})(x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = (x_m + y_m\sqrt{d})(x_n - y_n\sqrt{d})$$

$$x_{m-n} + \sqrt{d}\, y_{m-n} = x_n x_m - d y_m y_n + (x_n y_m - x_m y_n)\sqrt{d}$$

De donde

$$x_{m-n} = x_n x_m - d y_m y_n \quad \text{y} \quad y_{m-n} = x_n y_m - x_m y_n$$

Lema 6.1.6. $y_{m\pm1} = a y_m \pm x_m$ y $x_{m\pm1} = a x_m \pm d y_m$

Demostración. Tomamos $n = 1$ en el lema anterior y como

$$x_1 + y_1\sqrt{d} = a + \sqrt{d}$$

tenemos

$$x_1 = a \ , \quad y_1 = 1$$

Lema 6.1.7. $(x_n, y_n) = 1$

Demostración. Si $q \mid x_n$ y $q \mid y_n$ entonces $q \mid (x_n^2 - d y_n^2)$ i.e. $q \mid 1$.

Lema 6.1.8. $y_n \mid y_{nk}$.

Demostración. Para $k=1$ se cumple. Supongamos que $y_n \mid y_{nm}$. Vamos a demostrar que $y_n \mid y_{n(m+1)}$.

$$\begin{aligned} y_{n(m+1)} &= y_{nm+n} \\ &= y_{nm} x_n + y_n x_{nm} \end{aligned}$$

Como $y_n | y_n$ y $y_n | y_{nm}$, $y_n | y_{n(m+1)}$

Lema 6.1.9. $y_n | y_t$ si y solo si $n | t$.

Demostración. El lema anterior de la implicación en una dirección. Ahora, supongamos que $y_n | y_t$ y $n \nmid t$ Entonces $t = nq + r$ con $0 < r < n$. Por el lema 6.1.5.

$$y_t = y_{nq+r}$$

$$= y_{nq} x_r + y_r x_{nq}$$

Como $y_n | y_{nq}$ entonces $y_n | y_r x_{nq}$. Pero $(x_{nq}, y_n) = 1$ (si $d | x_{nq}$ y $d | y_n$, como $y_n | y_{nq}$ entonces $d | y_{nq}$; pero $(x_{nq}, y_{nq}) = 1$, y por lo tanto $d = 1$) entonces $y_n | y_r$. Como $r < n$ entonces $y_r < y_n$ (Lema 6.1.6). Esta es una contradicción.

Lema 6.1.10. $y_{nk} \equiv k x_n^{k-1} y_n \pmod{y_n^3}$.

Demostración. $x_{nk} + y_{nk}\sqrt{d} = [(a + \sqrt{d})^n]^k = (x_n + y_n\sqrt{d})^k$

$$= \sum_{j=0}^{k} \binom{k}{j} x_n^{k-j} y_n^j d^{\frac{j}{2}}$$

Así

$$y_{nk} = \sum_{\substack{j=1 \\ j \text{ impar}}}^{k} \binom{k}{j} x_n^{k-j} y_n^j d^{\frac{j-1}{2}}$$

los términos para $j > 1$ son congruentes con 0 mod y_n^3.

Por lo tanto

$$\sum_{\substack{j=1 \\ j \text{ impar}}}^{k} \binom{k}{j} x_n^{k-j} y_n^j d^{\frac{j-1}{2}} \equiv k\, x_n^{k-1} y_n \mod y_n^3$$

Es decir

$$y_{nk} \equiv k\, x_n^{k-1} y_n \mod y_n^3$$

Lema 6.1.11. $y_n^2 \mid y_{ny_n}$.

Demostración. Sea $k = y_n$ en el lema anterior; tenemos $y_{ny_n} \equiv y_n^2\, x_n^{y_n-1} \mod y_n^3$

y de aquí $y_{ny_n} = y_n^2 (x_n^{y_n-1} + ty_n)$

es decir y_n^2 / y_{ny_n}

Lema 6.1.12. Si y_n^2 / y_t entonces $y_n \mid t$.

Demostración. Si $y_n^2 | y_t$ entonces $y_n | y_t$ y por el lema 6.1.9 $n | t$. Sea $t = nk$. Usando el lema 6.1.10, $y_n^2 | k x_n^{k-1} y_n$, es decir $y_n | k x_n^{k-1}$; pero como $(x_n, y_n) = 1$, entonces $y_n | k$ y por lo tanto $y_n | t$.

Lema 6.1.13. $x_{n+1} = 2a\, x_n - x_{n-1}$ y $y_{n+1} = 2a y_n - y_{n-1}$.

Demostración. Por el lema 6.1.6

$$x_{n+1} = a x_n + d y_n \qquad y_{n+1} = a y_n + x_n$$

y

$$x_{n-1} = a x_n - d y_n \qquad y_{n-1} = a y_n - x_n$$

Sumando tenemos:

$$x_{n+1} + x_{n-1} = 2a x_n$$

$$y_{n+1} + y_{n-1} = 2a y_n$$

Así,

$$x_{n+1} = 2a x_n - x_{n-1}$$

$$y_{n+1} = 2a y_n - y_{n-1}$$

Estas dos ecuaciones junto con los valores iniciales $x_0 = 1$, $x_1 = a$, $y_0 = 0$, $y_1 = 1$ determinan los valores

de todas las x_n' s y y_n' s .

Muchas propiedades de estas sucesiones son fácilmente establecidas examinándolas para $n = 0, 1$ y usando estas ecuaciones para probar que la propiedad para $n + 1$ puede ser inferida de su validez para n y $n - 1$.

Enseguida vemos algunos ejemplos sencillos pero importantes.

Lema 6.1.14. $y_n \equiv n \mod(a-1)$.

Demostración. Para $n = 0, 1$ vale. Vamos a proceder inductivamente usando que $a \equiv 1 \mod a - 1$. Tenemos

$$\begin{aligned} y_{n+1} &= 2ay_n - y_{n-1} \\ &\equiv 2n - (n-1) \mod a - 1 \\ &= n + 1 \end{aligned}$$

Lema 6.1.15. Si $a \equiv b \mod C$ entonces $x_n(a) \equiv x_n(b) \mod C$ y $y_n(a) \equiv y_n(b) \mod C$.

Demostración. Para $n = 0, 1$ vale. Supongamos que

$$x_n(a) \equiv x_n(b) \mod C \qquad y_n(a) \equiv y_n(b) \mod C$$

y

$$x_{n-1}(a) \equiv x_{n-1}(b) \mod C \qquad y_{n-1}(a) \equiv y_{n-1}(b) \mod C$$

$$\begin{aligned} x_{n+1}(a) &= 2ax_n(a) - x_{n-1}(a) \\ &\equiv 2bx_n(b) - x_{n-1}(b) \mod C \\ &= x_{n+1}(b) \end{aligned}$$

$$\begin{aligned} y_{n+1}(a) &= 2ay_n(a) - y_{n-1}(a) \\ &\equiv 2by_n(b) - y_{n-1}(b) \mod C \\ &= y_{n+1}(b) \end{aligned}$$

<u>Lema 6.1.16</u>. Cuando n es par, y_n es par y cuando n es impar, y_n es impar.

<u>Demostración</u>. $y_{n+1} = 2ay_n - y_{n-1}$

$$\equiv y_{n-1} \mod 2$$

Así que, cuando n es par,

$$y_n \equiv y_0 \mod 2$$

$$= 0$$

y cuando n es impar

$$y_n \equiv y_1 \pmod 2$$

$$= 1.$$

<u>Lema 6.1.17.</u> $x_n(a) - y_n(a)(a-y) \equiv y^n \pmod{2ay-y^2-1}$.

<u>Demostración.</u> $x_0 - y_0(a-y) = 1$ y $x_1 - y_1(a-y) = y$

Así que el resultado vale para $n = 0$ y $n = 1$

Por el lema 6.1.13,

$$x_{n+1} - y_{n+1}(a-y) = (2ax_n - x_{n-1}) - (2ay_n - y_{n-1})(a-y)$$

$$= 2a[x_n - y_n(a-y)] - [x_{n-1} - y_{n-1}(a-y)]$$

Por hipótesis de inducción tenemos

$$x_n - y_n(a-y) \equiv y^n \pmod{(2ay-y^2-1)}$$

$$x_{n-1} - y_{n-1}(a-y) \equiv y^{n-1} \pmod{(2ay-y^2-1)}$$

Por lo tanto

$$x_{n+1} - y_{n+1}(a-y) \equiv 2ay^n - y^{n-1} \pmod{(2ay - y^2 - 1)}$$

$$= y^{n-1}(2ay - 1)$$

$$\equiv y^{n-1}y^2 \pmod{(2ay-y^2-1)}$$

$$= y^{n+1}$$

Lema 6.1.18. Para toda n, $y_{n+1} > y_n \geq n$.

Demostración. Por el lema 6.1.6, $y_{n+1} > y_n$. Ahora, tenemos que:

$$y_0 = 0 \geq 0$$

Supongamos que

$$y_n \geq n.$$

$$y_{n+1} = ay_n + x_n \geq an + x_n$$

$$> an > n + 1 .$$

Lema 6.1.19. Para toda n,

$$x_{n+1}(a) > x_n(a) \geq a^n \quad y \quad x_n(a) \leq (2a)^n$$

Demostración. Por lo lemas 6.1.6 y 6.1.13

$$x_n(a) < a\, x_n(a) \leq x_{n+1}(a) \leq 2a x_n(a)$$

Falta demostrar que

$$(2a)^n \geq x_n(a) \geq a^n$$

Para $n = 0$, se cumple. Supongamos que vale para n.

$$x_{n+1}(a) \geq a x_n(a) \geq a a^n = a^{n+1}$$

$$x_{n+1}(a) \leq 2a x_n(a) \leq 2a(2a)^n = (2a)^{n+1}$$

$$x_{n+1}(a) \leq 2a x_n(a) \leq 2a(2a)^n = (2a)^{n+1}$$

Lema 6.1.20. $x_{2n\pm j} \equiv - x_j \pmod{x_n}$

Demostración. Por el lema 6.1.5

$$\begin{aligned} x_{2n\pm j} &= x_n x_{n\pm j} + d y_n y_{n\pm j} \\ &= x_n x_{n\pm j} + d y_n (x_n y_j \pm y_n x_j) \\ &\equiv d y_n (x_n y_j \pm y_n x_j) \pmod{x_n} \\ &\equiv \pm d y_n (y_n x_j) \pmod{x_n} \\ &= \pm d y_n^2 x_j \\ &= (x_n^2 - 1)\, x_j \\ &\equiv - x_j \pmod{x_n} \end{aligned}$$

Lema 6.1.21. $x_{4n\pm j} \equiv x_j \pmod{x_n}$.

Demostración. Por el lema 6.1.20

$$\begin{aligned} x_{4n\pm j} = x_{2n+(2n\pm j)} &\equiv - x_{2n\pm j} \pmod{x_n} \\ &\equiv x_j \pmod{x_n} \end{aligned}$$

Lema 6.1.22. Sea $x_i \equiv x_j \mod x_n$, $i \leq j \leq 2n$, $n > 0$. Entonces $i = j$ a menos que $a = 2$, $n = 1$, $i = 0$, $j = 2$.

Demostración. Primero supongamos que x_n es impar y y sea $q = \frac{x_n - 1}{2}$ (Note que no puede ser que $n = 1$ y $a = 2$ pues $x_n(a) = x_1(2) = 2$ es par).

Entonces los números $-q, -q+1, -q+2, \ldots, 0, 1, \ldots, q-1, q$ son los representantes de todas las clases de equivalencia del conjunto $\mathbb{Z}x_n$. Usando el lema 6.1.6.

$$x_{n-1} \leq \frac{x_n}{a} \leq \frac{1}{2} x_n$$

así que $x_{n-1} \leq q$. También por el lema 6.1.20, los números

$$x_{n+1}, x_{n+2}, \ldots, x_{2n-1}, x_{2n}$$

son conguentes módulo x_n, respectivamente a:

$$-x_{n-1}, -x_{n-2}, \ldots, -x_1, -x_0 = -1$$

Así que, los números $x_0, x_1, \ldots, x_{2n}$ son mutuamente incongruentes módulo x_n. Esto nos da el resultado. Ahora supongamos que x_n es par, y sea $q := \frac{x_n}{2}$. En este caso, los números $-q+1, -q+2, \ldots, -1, 0, 1, \ldots, q$ son los

representantes de las clases de equivalencia del conjunto $\mathbb{Z}x_n$. Como antes $x_{n-1} \leq q$. Entonces tendremos el resultlado como arriba, a menos que $x_{n-1} = q = \frac{x_n}{2}$, esto es,

$$x_{n+1} \equiv -q \mod x_n$$

en cuyo caso $i = n - 1$, $j = n + 1$. Pero por el lema 6.1.6,

$$x_n = ax_{n-1} + dy_{n-1}$$

pero tenemos que

$$x_n = 2x_{n-1}$$

entonces $a = 2$ y $y_{n-1} = 0$, *i.e.*, $n=1$. Así el resultado puede fallar solamente para $a = 2$, $n = 1$, $i = 0$ y $j = 2$.

Lema 6.1.23. Sea $x_j \equiv x_i \mod x_n$, $n > 0$, $0 < i \leq n$, $0 \leq j < 4n$, entonces, o $j = i$ o $j = 4n - i$.

Demostración. Primero supongamos que $j \leq 2n$. Entonces por el lema 6.1.22, $j = i$ a menos que suceda el caso excepcional. Como $i > 0$ el caso excepcional sucedería solo si $j = 0$. Pero entonces tendríamos $i = 2 \leq 1=n$. El otro caso es que $j > 2n$ y sea $\overline{j} = 4n-j$ con $0 < \overline{j} < 2n$. Por el lema 6.1.21 tenemos

$$x_{\bar{j}} \equiv x_j \equiv x_i \qquad \text{mod } x_n$$

De nuevo $\bar{j} = i$ a menos que suceda el caso excepcional. Pero este no puede suceder pues $i, \bar{j} > 0$.

Lema 6.1.24. Si $0 < i \leq n$ y $x_i \equiv x_j \mod x_n$, entonces $j \equiv \pm i \mod 4n$.

Demostración. Escribimos

$$j = 4nq + \bar{j}, \quad 0 \leq j < 4n$$

Por el lema 6.1.21,

$$x_i \equiv x_j \equiv x_{\bar{j}} \qquad \text{mod } x$$

Por el lema 6.1.23,

$$i = j \quad \text{o} \quad i = 4n - \bar{j}$$

Así que

$$j \equiv j \equiv \pm i \qquad \text{mod } 4n$$

6.2. LA FUNCION EXPONENCIAL

Considere el sistema de ecuaciones diofantinas:

I $\quad x^2 - (a^2 - 1)\, y^2 = 1$

II $\quad u^2 - (a^2 - 1)v^2 = 1$

III $\quad s^2 - (b^2 - 1)t^2 = 1$

IV $\quad v = ry^2$

V $\quad b = 1 + 4py = a + qu$

VI $\quad s = x + cu$

VII $\quad t = k + 4(d - 1)y$

VIII $\quad y = k + e - 1$

Entonces probaremos:

Teorema 6.2.1. Dadas a, x, k, $a > 1$, el sistema I-VIII tiene solución en las variables y, u, v, s, t, b, r, p, q, c, d, e si y solo si $x = x_k(a)$.

Demostración. Primero damos una solución del sistema I-VIII. Por V, $b > a > 1$. Entonces I, II y III implican por el lema 6.1.4 que existen i, j, $n > 0$ tales que

$$x = x_i(a) \qquad y = y_i(a)$$

$$u = x_n(a) \qquad v = y_n(a)$$

$$s = x_j(b) \qquad t = y_j(b)$$

Por IV, $y \leqslant v$ y de aquí $i \leqslant n$; V y VI implican que

$$b \equiv a \mod x_n(a)$$

y

$$x_j(b) \equiv x_i(a) \mod x_n(a)$$

y por el lema 6.1.15 tenemos

$$x_j(b) \equiv x_j(a) \mod x_n(a)$$

Esto es,

$$x_j(a) \equiv x_i(a) \mod x_n(a)$$

Por el lema 6.1.24 tenemos que

(1) - - - - - - $j \equiv \pm i \mod 4n$

La ecuación IV implica que y^2/v, es decir

$$(y_i(a))^2 / y_n(a)$$

y por el lema 6.1.12,

$$y_i(a)/n$$

y por (1) tenemos

(2) - - - - - - $j \equiv \pm i \mod 4y_i(a)$

Por la ecuación V,

$$b \equiv 1 \mod 4y$$

y por el lema 6.1.14,

$$y_j(b) \equiv j \mod (b-1) \text{ es decir}$$

(3) - - - - - - $y_j(b) \equiv j \mod 4y_i(a)$

Por la ecuación VII,

$$t \equiv k \mod 4(d-1)y, \text{ es decir}$$

(4) - - - - - - $y_j(b) \equiv k \mod 4y_i(a)$

Combinando (2), (3) y (4) tenemos,

(5) - - - - - - $k \equiv \pm i \mod 4y_i(a)$

La ecuación VIII conduce a que $y \geq k$; y por el lema 6.1.18 tenemos

$$y_i(a) \geq i$$

ya que los números

$$-2y+1, -2y+2, \ldots, -1, 0, 1, 2, \ldots 2y$$

forman un conjunto completo de residuos mutamente incongruentes módulo $4y$, estas desigualdades prueban que $k = i$. De aquí, tenemos

$$x = x_i(a) = x_k(a)$$

Ahora, inversamente, sea $x = x_k(a)$ póngase $y = y_k(a)$ de suerte que (I) vale. Sea $m = 2ky_k(a)$ y sea $u = x_m(a)$, $v = y_m(a)$. Entonces (II) se satisface. Por los lemas 6.1.9 y 6.1.11

$$y^2 | v$$

De aquí podemos elegir n de tal manera que IV se cumpla. Más aún, por el lema 6.1.16 $v = y_m$ es par, así que u es impar. Por el lema 6.1.7, $(u,v) = 1$, así que $(u, 4vy) = 1$ (sea p un divisor primo de u y $4vy$; como $p \nmid v$ entonces $p|4y$ y entonces $p|y$ puesto que u es impar; pero como $y^2|v$ entonces $y|v$ y de aquí $p|v$). Así por el teorema del residuo chino podemos encontrar

$$bo \equiv 1 \mod 4y$$

$$bo \equiv a \mod u$$

ya que $bo + 4juy$ también satisface esta congruencia - podemos encontrar b, p y q que satisfagan V. III se satisface poniendo $s = x_k(b)$, $t = y_k(b)$ ya que $b > a$,

$s = x_k(b) > x_k(a) = x$. Por el lema 6.1.15 y usando V tenemos que como

$$b \equiv a \mod u$$

entonces

$$x_k(b) \equiv x_k(a) \mod u \qquad i.e.$$

$$s \equiv x \mod u$$

así podemos elegir c de tal forma que VI se satisfaga. Por el lema 6.1.18, $t \geqslant k$ y por el lema 6.1.14, $y_k(b) \equiv k \mod(b - 1)$ y de aquí usando V

$$t \equiv k \mod 4y$$

así podemos elegir d, tal que VII se cumpla.

Nuevamente usando el lema 6.1.18, $y \geqslant k$; así se puede obtener VIII poniendo $e = y - k + 1$.

Corolario 6.2.2. La función

$$g(z,k) = x_k(z + 1)$$

es diofantina.

Demostración. Agregamos al sistema I-VIII, la ecuación

(A) - - - - - - $a = z + 1$.

Por el teorema anterior, el sistema A.I-VIII tiene solución si y solo si $x - x_k(a) = x_k(z + \ ) = g(a,k)$. Así, podemos dar una definición diofantina de g de la forma usual: sumando los cuadrados de los nueve polinomios.

Ahora, ya podemos demostrar:

Teorema 6.2.3. La función exponencial

$$h(n,k) = n$$

es diofantina.

Antes de demostrar este teorema, prcbaremos una desigualdad:

Lema 6.2.4. Si $a > y^k$ entonces $2ay - y^2 - 1 > y^k$.

Demostración. Sea $g(y) = 2ay - y^2 - 1$. Entonces, como $a \geq 2$, tenemos

$$g(1) = 2a - 2 \geq a \ .$$

Ahora, para

$$1 \leq y < a,$$

$$g'(y) = 2a-2y > 0 \quad \text{ya que} \quad a > y$$

Como $g'(y) > 0$ tenemos que $g(y)$ es creciente para

$1 \leqslant y < a$:

$$a \leqslant g(1) \leqslant g(y) .$$

Entonces si $a > y^k > y$ tenemos

$$g(y) \geqslant a$$

es decir

$$2ay - y^2 - 1 \geqslant a > g^k$$

Ahora, agregamos al sistema I - VIII, las ecuaciones:

IX $(x - y(a-n)-m)^2 = (\ell - 1)^2 (2an-n^2-1)^2$

X $m + g = 2an - n^2 - 1$

XI $w = n + h = k + \ell$

XII $a^2 - (w^2 -) (w - 1)^2 z^2 = 1$

Teorema 6.2.5. $m = n^k$ si y solo si las ecuaciones I - XII tienen solución en las restantes variables.

Demostración. Supongamos que I - XII tienen solución. por XI, $w > 1$. De aquí que $(w - 1) z > 0$ y entoncees por XII, $a > 1$. Así, aplicando el teorema 6.2.1 se sigue que $x = x_k(a)$, $y = y_k(a)$. Por IX y aplicando el le-

ma 6.1.17 tenemos que

$$m = n^k \qquad \text{mod}\,(2an - n^2 - 1)$$

XI lleva a $k, n < w$. Por XII y usando el lema 6.1.4, tenemos que para algún j, $a = x_j(w)$, $(w - 1)z = y_j(w)$. Por el lema 6.1.14,

$$y_j(w) \equiv j \qquad \text{mod } w\text{-}1$$

y de aquí

$$j \equiv 0 \qquad \text{mod } w\text{-}1$$

$$j \geqslant w\text{-}1$$

De manera que por el lema 6.1.19

$$a = x_s(w) \geqslant x_{w-1}(w) \geqslant w^{w-1} > n^k$$

Ahora, por X, $m < 2an - n^2 - 1$

y por el lema 6.2.4.

$$2an - n^2 - 1 > n^k \qquad \text{pues} \quad a > n^k$$

De

$$m \equiv n^k \qquad \text{mod}\,(2an - n^2 - 1)$$

$$m < 2an - n^2 - 1$$

$$n^k < 2an - n^2 - 1$$

tenemos que

$$m = n^k$$

Inversamente, supongamos que $m = n^k$, Debemos encontrar soluciones de I-XII. Elegimos cualquier número w tal que $w > n$ y $w > k$. Sea $a = x_{w-1}(w)$, así que $a > 1$. Por el lema 6.1.14, tenemos

$$y_{w-1}(w) \equiv w - 1 \qquad \text{mod } w - 1$$

Por lo tanto, escribimos

$$y_{w-1}(w) = z(w-1)$$

Así, XII se satisface. XI puede satisfacerse, poniendo $h = w - n$, $\ell = w - k$. Como antes, tenemos que $a > n^k$, así que nuevamente por el lema 6.2.4

$$m = n^k < 2an - n^2 - 1$$

y entonces X se cumple. Poniendo $x = x_k(a)$, $y = y_k(a)$, el lema 6.1.17 permite definir δ tal que

$$x - y(a-n) - m = \pm(\delta - 1)(2an - n^2 - 1)$$

así que IX se cumple. Finalmente I-VIII pueden satisfacerse por el teorema 6.2.1..

6.3. EL LENGUAJE DE LOS PREDICADOS DIOFANTINOS

Ahora que hemos probado que la función exponencial es diofantina, podemos estudiar otras funciones y conjuntos. Como un ejemplo, sea

$$h(u,v,w) = u^{v^w}$$

Lo que se pretende ver, es que h es diofantina:

$$y = u^{v^w} \iff (\exists z)[y = u^z \wedge z = v^w]$$

Por el teorema 6.2.5 existen dos polinomios P,Q tales que

$$y = u^z \iff (\exists r_1,\ldots,r_n)[P(y,u,z,r_1,\ldots,r_n) = 0]$$

y

$$z = v^w \iff (\exists s_1,\ldots,s_m)[Q(z,v,w,s_1,\ldots,s_m) = 0]$$

Por lo tanto

$$y = u^{v^w} \iff (\exists r_1,\ldots,r_n,s_1,\ldots,s_m)[P^2(y,u,z,r_1,\ldots,r_n) + Q^2(z,v,w,s_1,\ldots,s_m) = 0]$$

Este procedimiento es perfectamente general: expresiones, las cuales, las conocemos como conjuntos diofantinos pueden combinarse usando las operaciones lógicas $\wedge$ y $\exists$; las expresiones resultantes son nuevamente con

juntos diofantinos (tales expresiones, muchas veces, son llamados "predicados diofantinos"). En este lenguaje es también permisible usar el símbolo lógico $\vee$ para *"o"* - ya que

$$(\exists r_1, \ldots, r_n)[P_1 = 0] \vee (\exists s_1, \ldots, s_m)[P_2 = 0]$$

$$\Longleftrightarrow$$

$$(\exists r_1, \ldots, r_n, s_1, \ldots, s_m)[P_1 P_2 = 0]$$

Tres funciones diofantinas muy importantes están dadas en el siguiente teorema:

Teorema 6.3.1. Las siguientes funciones son diofantinas:

$$\delta(n,k) = \binom{n}{k}, \quad g(n) = n!, \quad h(a,b,y) = \prod_{k=1}^{y} (a+bk)$$

Para demostrar este teorema, usaremos la notación $[\alpha]$ donde α es un número real y significa que $[\alpha]$ es el único entero tal que

$$[\alpha] \leq \alpha < [\alpha] + 1$$

Lema 6.3.2. Para $0 < k \leq n$ y $u > 2^n$ se tiene

$$\left[\frac{(u+1)^n}{u^k}\right] = \sum_{i=k}^{n} \binom{n}{i} u^{i-k} .$$

Demostración.

$$\frac{(u+1)^n}{u^k} = \sum_{i=0}^{n} \binom{n}{i} u^{i-k} = S + R$$

donde

$$S = \sum_{i=k}^{n} \binom{n}{i} u^{i-k} \quad y \quad R = \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k}$$

Entonces S es entero y $R < 1$. Por lo tanto

$$S \leq \frac{(u+1)^n}{u^k} < S + 1$$

y por lo tanto

$$S = \left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor$$

Lema 6.3.3. Para $0 < k \leq n$ y $u > 2^n$,

$$\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \equiv \binom{n}{k} \mod u$$

Demostración. En el lema anterior, todos los términos de la suma para los cuales $i > k$ son divisible por u.

Lema 6.3.4. $\beta(n,k) = \binom{n}{k}$ es diofantina.

Demostración. Ya que

$$\binom{n}{k} < \sum_{i=0}^{n} \binom{n}{i} = 2^n < u$$

el lema 6.3.3. determina $\binom{n}{k}$ como el único entero positivo congruente con

$$\left[\frac{(u+1)^n}{u^k}\right]$$

módulo u y menor que u.

Así, tenemos:

$$z = \binom{n}{k} \iff (\exists\, u,v,w)[\, v = 2^n \wedge u > v \cdot \wedge$$

$$w = \left[\frac{(u+1)^n}{u^k}\right] \wedge z \equiv w \bmod u \wedge z < u]$$

Para demostrar que $\beta(n,k) = \binom{n}{k}$ es diofantina basta ver que cada una de las expresiones de arriba, separadas por el $\cdot\wedge$ son diofantinas:

$v = 2^n$ es diofantina por el teorema 6.2.5

$u > v$ es diofantina pues $u > v \iff (\exists x)[\, u = v + x]$

$$z \equiv w \mod u \wedge z < u \iff (\exists y, x)[w = z + (x - 1)\, u \wedge u = z + y]$$

$$w = \left[\frac{(u+1)^n}{u^k}\right] \iff (\exists x, y, t)[t = u + 1 \wedge x = t^n \wedge y = u^k \wedge w \leq \frac{x}{y} < w + 1]$$

$$w \leq \frac{x}{y} < w + 1 \iff wy \leq x < wy + y$$

Lema 6.3.5. Si $n > (2x)^{x+1}$ entonces $x! = \left[\frac{n^x}{\binom{n}{x}}\right]$

Demostración. Sea $n > (2x)^{x+1}$

$$\frac{n^x}{\binom{n}{x}} = \frac{n^x\, x!}{n(n-1)\ldots(n - x + 1)}$$

$$< x! \left(\frac{1}{1 - \frac{x}{n}}\right)^x$$

Ahora $\dfrac{1}{1 - \frac{x}{n}} < 1 + \dfrac{2x}{n}$

y como $\left(1 + 2\,\dfrac{x}{n}\right)^x = \sum_{j=0}^{x} \binom{x}{j} \left(\dfrac{2x}{n}\right)^j$

$$< 1 + \frac{2x}{n} \sum \binom{x}{j}$$

$$< 1 + \frac{2x}{n}\, 2^x$$

tenemos:

$$\frac{n^x}{\binom{n}{x}} < x! \; \frac{1}{(1-\frac{x}{n})^x}$$

$$< \; x! \; (1 + \frac{2x}{n} \, 2^x)$$

$$< \; x! + \frac{(2x)^{x+1}}{n}$$

$$< \; x! + 1$$

Así

$$x! \leqslant \frac{n^x}{\binom{n}{x}} < x! + 1$$

Por lo tanto

$$\left[\frac{n^x}{\binom{n}{x}}\right] = x!$$

Lema 6.3.6. $\beta(n) = n!$ es diofantina.

Demostración. $m = n!$

$$\langle = \rangle$$

$$(\exists n, s, t, u, v) \; [s = 2x + 1 \wedge t = x + 1 \wedge n = s^t \wedge$$

$$u = n^n \wedge v = \binom{n}{n} \wedge m \leqslant \frac{u}{v} < m + 1]$$

Lema 6.3.7. Sea $bq \equiv a \mod M$.

Entonces $\prod_{k=1}^{y} (a + bk) \equiv b^y y! \binom{q+y}{y} \mod M$

Demostración. $b^y y! \binom{q+y}{y} = b^y y! \frac{(q+y)!}{y!q!}$

$$= b^y (q+y)(q+y-1)\ldots(q+1)$$

$$= \prod_{k=1}^{y} (bq+bk)$$

$$\equiv \prod_{k=1}^{y} (a+bk) \quad mod\ M$$

Lema 6.3.8. $h(a,b,y) = \prod_{k=1}^{y} (a+bk)$ es una función diofantina.

Demostración. En el lema anterior elegimos

$$M = b(a+by)^y + 1$$

Entonces $(M,b) = 1$ y $M > \prod_{k=1}^{y} (a + bk)$. Aquí la congruencia $bq \equiv a \mod M$ es resoluble para q y entonces $\prod_{k=1}^{y} (a+bk)$ está determinado como el único número el cual es congruente con $b^y y! \binom{q+y}{y} \mod M$ y menor que M; es decir:

$$z = \prod_{k=1}^{y} (a+bk)$$

$$\langle\Longrightarrow\rangle$$

$$(\exists M,p,q,r,s,t,u,v,w,x)\ [r = a+by \wedge s = r^y \wedge$$

$$M = bs + 1 \wedge bq = a + Mt \wedge u = b^y \wedge v = y! \wedge z < M \wedge$$

$$w = q + y \wedge x = \binom{w}{y} \wedge z + Mp = u\,v\,x]$$

Usando los resultados anteriores para la función exponencial, para $v = y!$ y para $x = \binom{w}{y}$ obtenemos el resultado.

La afirmación del teorema 6.3.1 está contenida en los lemas 6.3.4, 6.3.6 y 6.3.8.

6.4. CUANTIFICADORES ACOTADOS.

El lenguaje de los predicados diofantinos permite usar los símbolos lógicos $\wedge$, $\vee$ y $\exists$. Otras operaciones usadas por los lógicos son:

$\sim$ para "no"

$\forall x$ para "para toda x"

=> para "si...entonces..."

Sin embargo, como será claro mas tarde, el uso de cualquiera de estas operaciones puede llevar a expresiones las cuales definan conjuntos que no son diofantinos.

Existen también el cuantificador existencial acotado:

" $(\exists y)_{\leqslant x}$ ..." significa "$(\exists y)(y \leqslant x \wedge \ldots)$

y el cuantificador universal acotado:

" $(\forall y)_{\leqslant x}$ ..." significa "$(\forall y)(y \leqslant x \wedge \ldots)$

Se prueba que estas operaciones pueden adjuntarse al lenguaje de los predicados diofantinos; esto es, los conjuntos definidos por expresiones de este lenguaje extendido serán conjuntos diofantinos, *i. e*,

Teorema 6.4.1. Si P es un polinomio,

$$R = \{(y, x_1, \ldots, x_n) : (\exists z)_{\leqslant y} (\exists y_1, \ldots, y_m)[P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\}$$ y

$$S = \{(y, x_1, \ldots, x_n) : (\forall z)_{\leqslant y} (\exists y_1, \ldots, y_m)[P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\}$$ entonces R y S son diofantinas.

Demostración. Que R es diofantino, es trivial:

$$(y, x_1, \ldots, x_n) \in R \iff (\exists z, y_1, \ldots, y_m)\ (z \leqslant y \wedge P = 0)$$

La prueba de la otra parte del teorema es un poco más complicada.

Lema 6.4.2. $(\forall k)_{\leq y}\,(\exists y_1,\ldots,y_m)[P(y,k,x_1,\ldots,x_n,y_1,\ldots,y_m)=0]$

$$\Longleftrightarrow$$

$$(\exists u)(\forall k)_{\leq y}(\exists y_1,\ldots y_m)_{\leq u}[P(y,k,x_1,\ldots,x_n,y_1,\ldots,y_m) = 0]$$

Demostración. El lado derecho de la equivalencia implica trivialmente el lado izquierdo. Para demostrarlo recíprocamente supongamos que el lado izquierdo es verdadero para $y, x_1,\ldots,x_n$ dados. Entonces para cada $k = 1,2,\ldots,y$ existen números definidos $y_1^{(k)},\ldots,y_m^{(k)}$ para los cuales:

$$P(y,k,x_1,\ldots,x_n,y_1^{(k)},\ldots,y_m^{(k)}) = 0$$

Tomando u igual al máximo del conjunto

$$\{y_j^{(k)}:\ j = 1,\ldots,m\ ;\ k = 1,\ldots,y\}$$

tenemos que el lado derecho de la equivalencia también vale.

Lea 6.4.3. Sea $Q(y,u,x_1,\ldots,x_n)$ un polinomio con los propiedades:

i) $Q(y,u,x_1,\ldots,x_n) > u$

ii) $Q(y,u,x_1,\ldots,x_n) > y$

iii) $k \leq y$ y $y_1,\ldots,y_m \leq u \Rightarrow |P(y,k,x_1,\ldots,x_n,y_1,\ldots,y_m)| \leq Q(y,u,x_1,\ldots,x_n)$

Entonces

$$(\forall k)_{\leq y}(\exists y_1,\ldots,y_m)_{\leq u}\ [P(y,k,x_1,\ldots,x_n,\ y_1,\ldots,y_m)=0]$$

$$<==>$$

$$(\exists c,t,a_1,\ldots,a_n)[\,1+ct=\prod_{k=1}^{y}(1+kt)\ \wedge\ t=Q(y,u,x_1,\ldots,x_n)\,!\ \wedge$$

$$(1+ct)\,|\prod_{j=1}^{u}(a_1-j)\ \wedge\ldots\wedge\ (1+ct)\,|\prod_{j=1}^{u}(a_m-j)\quad P(y,c,x_1,\ldots,x_n,$$

$$a_1,\ldots,a_m)\ \equiv\ 0\mod 1+ct]$$

<u>Demostración</u>. La ventaja de este lema es que mientras que el lado derecho de la equivalencia parece el más complicado de los dos está libre de cuantificadores universales acotados. Primero damos la implicación en la dirección (<=).

Para cada $k = 1,\ldots,y$, sea p_k un factor primo de $1 + kt$. Sea $y_i^{(k)}$ el residuo cuando a_i es dividido por $p_k (i = 1,\ldots,m)$.

Se sigue que para cada k, i:

a) $\quad 1 \leq y_i^{(k)} \leq u$

b) $\quad P(y,k,x_1,\ldots,x_n,\ y_1^{(k)},\ldots,y_m^{(k)}) = 0$

Para demostrar a), note que $p_k \mid \prod_{j=1}^{u} (a_i - j)$; ya que p_k es primo, $p_k \mid (a_i - j)$ para alguna j. Esto es:

$$j \equiv a_i \mod p_k$$

$$\equiv y_i^{(k)} \mod p_k$$

y que $t = Q(y, u, x_1, \ldots, x_n)!$, (ii) implica que cada divisor de $1 + kt$ debe ser mayor que $Q(y, u, x_1, \ldots, x_n)$. Así, p_k es mayor que $Q(y, u, x_1, \ldots, x_n)$ y por (i) tenemos que $p_k > u$. De aquí que

$$j \leq u < p_k$$

Como $y_i^{(k)} < p_k$, entonces $y_i^{(k)} = j$. Para demostrar (b) note primero que

$$1 + ct \equiv 1 + kt \mod p_k$$

y de aquí

$$k \equiv c \mod p_k$$

Como ya tenemos que

$$y_i^{(k)} \equiv a_i \mod p_k$$

entonces

$$P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)}) \equiv P(y, c, x_1, \ldots, x_n, a, \ldots, a_m) \mod P_k$$

$$\equiv 0 \mod P_k$$

Finalmente

$$|P(y,k,x_1,\ldots,x_n,\ y_1^{(k)},\ldots,y_m^{(k)})| \leqslant Q(y,u,x_1,\ldots,x_n)$$

$$\leqslant p_k$$

Esto completa la prueba de la implicación (<=).

Para probar la implicación (⇒), sea $P(y,k,x_1,\ldots,x_n, y_1^{(k)},\ldots,y_m^{(k)}) = 0$ para cada $k = 1,\ldots,t$ donde $y_j^{(k)} \leqslant u$.

Sea

$$t = Q(y,u,x_1,\ldots,x_n)!$$

y ya que

$$\prod_{k=1}^{y}(1 + kt) \equiv 1 \qquad \mod t$$

podemos encontrar c tal que

$$1 + ct = \prod_{k=1}^{y}(1 + kt)$$

Ahora, queremos que para $1 \leqslant k < \ell < y$,

$$(1 + kt,\ 1 + \ell t) = 1$$

Sea $p \mid (1+ kt$ 0 y $p \mid (1+ \ell t)$ Entonces $p \mid (\ell-k)$ y así $< y$.

Pero como

$$Q(y,u,x_1,\ldots,x_n) > y$$

entonces $P \mid t$, lo cual es imposible. Así, los números

$1 + kt$, $1 \leqslant k < y$ son primos relativos por pares y po demos aplicar el Teorema Chino del Residuo: para cada i, $1 \leqslant i \leqslant m$, existe a_i tal que

$$a_i \equiv y_i^{(k)} \mod 1 + kt \qquad k = 1, 2, \ldots, y$$

Como antes, tenemos

$$k \equiv c \mod 1 + kt$$

entonces

$$P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)}) \mod 1+kt$$

$$\equiv 0 \mod 1 + kt$$

Ya que los números $1 + kt$ son primos relativos por pares y cada uno divide a $P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m)$, entonces también su producto, $i.e.$

$$P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0 \mod 1 + ct$$

Finalmente

$$a_i \equiv y_i^{(k)} \mod 1 + kt$$

$i.e.,$ $\quad 1 + kt \mid (a_i - y_i^{(k)})$

Ya que $\quad 1 \leqslant y_i^{(k)} \leqslant u$

$$1 + kt \mid \prod_{j=1}^{u} (a_i - j)$$

y nuevamente como los $1 + kt$ son primos relativos por pares

$$(1+ct) \mid \prod_{j=1}^{u} (a_i - j)$$

Ahora, es fácil completar la prueba del teorema 6.4.1 usando los lemas 6.4.2 y 6.4.3. Primero encontramos un polinomio Q que satisfaga (i), (ii) y (iii) del lema 6.4.3. Esto es fácil hacerlo:

Sea

$$P(y,k,x_1,\ldots,x_n,y_1,\ldots,y_m) = \sum_{r=1}^{N} t_r$$

donde cada t_r tiene la forma

$$t_r = cy^a k^b x_1^{q_1} x_2^{q_2},\ldots,x_n^{q} y_1^{s_1},\ldots y_r^{s_r}$$

para c un entero positivo o negativo. Sea

$$u_r = |c| y^{a+b} x_1^{q_1},\ldots,x_n^{q_n} u^{s_1+},\ldots,+s_r$$

y sea

$$Q(y,u,x_1,\ldots,x_n) = u + y + \sum_{r=1}^{N} u_r$$

Entonces (i), (ii) y (iii) del lema 6.4.3, son trivialmente satisfechas

(i) $Q(y,u,x_1,\ldots,x_n) = u + y + \sum_{r=1}^{N} u_r > u$

(ii) $Q(y,u,x_1,\ldots,x_n) = u + y + \sum_{r=1}^{N} u_r > y$

(iii) Si $k \leq y$ y $y_1,\ldots,y_m \leq u$ entonces

$$|c|y^a k^b x_1^{q_1},\ldots,x_1^{q_n} y_1^{s_1},\ldots,y_r^{s_r} \leq |c|y^{a+b} x_1^{q_1}\ldots x_n^{q_n} u^{s_1+\ldots+s_r}$$

i.e. $|t_r| \leq u_r$

$$|\sum_{r=1}^{n} t_r| \leq \sum_{r=1}^{n} |t_r| \leq \sum_{r=1}^{n} u_r$$

y por lo tanto

$$|\sum_{r=1}^{n} t_r| \leq u + y + \sum u_r$$

es decir

$$|P(y,k,x_1,\ldots,x_n,y_1,\ldots,y_m)| \leq Q(y,u,x_1,\ldots,x_n)$$

Como se cumplen (i), (ii) y (iii) tenemos:

$$(\forall k)_{\leq y}(\exists y_1,\ldots,y_m)[P(y,k,x_1,\ldots,x_n,y_1,\ldots,y_m) = 0]$$

$$\langle\!=\!\rangle$$

$$(\exists u,c,t,a_1,\ldots,a_m)[1+ct=\prod_{k=1}^{y}(1+kt) \wedge t = Q(y,u,x_1,\ldots,xn)]$$

$$\wedge\ (1 + ct)\quad \Big|\prod_{j=1}^{u}(a_1 - j)\wedge \ldots\ldots \wedge (1+ct)\Big|\prod_{j=1}^{u}(a_m - j)\wedge P \equiv 0 \mod 1 + ct]$$

$$<==>$$

$$(\exists u, c, t, a_1, \ldots, a_m, e, \delta, g_1, \ldots, g_m, h, \ldots, h_m)[\, e = 1+ct \wedge$$

$$e = \prod_{k=1}^{y}(1+kt) \wedge \delta = Q(y, u, x_1, \ldots, x_m) \wedge t = \delta! \wedge$$

$$g_1 = a_1 - u - 1 \wedge g_2 = a_2 - u - 1 \wedge \ldots \wedge g_m = a_m - u - 1 \wedge$$

$$h_1 = \prod_{k=1}^{u}(g_1 + k) \wedge \ldots \wedge h = \prod_{k=1}^{u}(g_m + k) \wedge e \mid h_1 \wedge e \mid h_1 \wedge$$

$$e \mid h_2 \wedge \ldots \wedge e \mid h_m \wedge \ell = P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \wedge$$

$$e \mid \ell]$$

y esto es diofantino por el teorema 6.3.1.

6.5. ¿CUALES CONJUNTOS Y FUNCIONES NO SON DIOFANTINOS?

Hasta aquí es claro que los métodos disponibles son completamente generales. Es por esto que surge la siguiente pregunta: ¿Cuáles conjuntos o funciones "razonables" no son diofantinos?

Uno de los principales resultados de este capítulo es:

Teorema 6.5.1. Una función es diofantina si y solo si es recursiva.

Demostración. Supongamos que ϕ es diofantina. Entonces:

$$y = \phi(x_1,\ldots,x_m) \iff (\exists t_1,\ldots,t_m)[P(x_1,\ldots,x_n,y,t_1,\ldots,t_m) =$$

$$Q(x_1,\ldots,x_n,y,\ t_1,\ldots,t_m)]$$

donde P y Q son polinomios con coeficientes enteros positivos. Entonces por el Teorema de la Sucesión de Números:

$$\phi(x_1,\ldots,x_n) = S(1,\min_u[P(x_1,\ldots,x_n,S(1,u),\ldots,S(m+1,u)) =$$

$$Q(x_1,\ldots,x_n,S(1,u),\ldots,S(m+1,u))])$$

ya que $P,Q,S(i,u)$ son recursivas, ϕ también lo es (usando composición y minimización). Para demostrar el inverso: sabemos que $S(i,u)$ es diofantina, las otras funciones iniciales son trivialmente diofantinas. Así que es suficiente probar que las funciones diofantinas son cerradas bajo Composición, Recursión Primitiva y Minimización:

Composición. Si

$$h(x_1,\ldots,x_n) = \phi(g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots x_n))$$

donde ϕ, $g_1,\ldots,g_m$ son diofantinas entonces h también lo es ya que

$$u=h(x_1,\ldots.x_m)\Leftrightarrow(\exists t_1,\ldots,t_m)[t_1=g_1(x_1,\ldots,x_n)\wedge\ldots\wedge tm =$$

$$g_m(x_1,\ldots,x_n)\wedge y = \phi(t_1,\ldots,t_m)]$$

Recursión Primitiva.

Si $h(x_1,\ldots,x_n,1) = \phi(x_1,\ldots,x_n)$

y $h(x_1,\ldots,x_n,t+1)=g(t,h(x_1,..,x_n,t),x_1,\ldots,x_n)$

donde ϕ y g son diofantinas entonces usando el Teorema de la Sucesión de Números

$$y = h(x_1,\ldots,x_n,z) \iff (\exists u)\{S(1,u)=h(x_1,\ldots,x_n,1) \wedge (\forall t)\leq z$$

$$[t=z \vee S(t+1.u)=g(t,S(t,u),x_1,\ldots,x_n)]$$

$$\wedge S(z,u) = y\}$$

$$\iff (\exists u)\{(\exists v)[v = S(1,u) \wedge v = h(x_1,\ldots,$$

$$x_n,1)] \wedge (\forall t)_{\leq z}[t=z \vee (\exists w)(w =$$

$$S(t+1,u)) \wedge w = g(t,S(t,u),x_1,\ldots,x_n)]$$

$$\wedge y = S(z,u)\}$$

Por lo tanto, usando el teorema 6.4.1; h es diofantina.

Minimización.

Si $h(x_1,\ldots,x_n) = \min_y \{\delta(x_1,\ldots,x_n,y)=g(x_1,\ldots,x_n,g)\}$ donde δ, g son diofantinas entonces h también lo es ya que

$$y=h(x_1,\ldots,x_n) \iff \{(\exists z)[z=\delta(x_1,\ldots,x_n,y) \wedge z=g(x_1,\ldots,x_n,y)]$$

$$\wedge (t)_{\leq y}[t=y \vee (\exists u,v)(u=\delta(x_1,\ldots,x_n,t)$$

$$\wedge v = g(x_1,\ldots,x_n,t) \wedge (u<v \vee v < u))]\}$$

Ahora vamos a responder la pregunta que nos hicimos desde el principio del capítulo: ¿cuáles conjuntos no son diofantinos?

Definición.6.5.1. Un conjunto S de n-adas de enteros positivos es recursivamente numerable si existen funciones recursivas $f(x_1,\ldots,x_n)$ y $g(x_1,\ldots,x_n)$ tales que

$$S = \{(x_1,\ldots,x_n):(\exists x)[f(x,x_1,\ldots,x_n)=g(x,x_1,\ldots,x_n)]\}$$

Teorema 6.5.2. Un conjunto S es diofantino si y solo si es recursivamente numerable.

Demostración. Si S es diofantino existen polinomios P y Q con coeficientes positivos tal que:

$$(x_1,\ldots,x_n)\in S \iff (\exists y_1,\ldots,y_m)[P(x_1,\ldots,x_n,y_1,\ldots,y_m)=Q(x_1,\ldots,x_n,y_1,\ldots,y_m)]$$

$$\iff (\exists u)[P(x_1,\ldots,x_n,S(1,u),\ldots,S(m,u)) =$$

$$Q(x_1,\ldots,x_n, S(1, u),\ldots, S(m, u))]$$

así que S es recursivamente numerable.

Inversamente, si S es recursivamente numerable, exis
n funciones recursivas $f(x,x_1,\ldots,x_n)$, $g(x,x_1,\ldots,x_n)$
les que:

$$(x_1,x_2,\ldots,x_n) \in S \iff (\exists x)[f(x,x_1,\ldots,x_n)=g(x,x_1,\ldots,x_n)]$$

$$\iff (\exists x,z)[z=f(x,x_1,\ldots,x_n) \wedge z=g(x,x_1,\ldots,x_n)]$$

Así, por el teorema 6.5.1, S es diofantino.

.6. UN CONJUNTO UNIVERSAL DIOFANTINO

Daremos una enumeración de los conjuntos diofantinos
e enteros positivos.

Cualquier polinomio con coeficientes enteros positi-
os se puede obtener del uno y variables con sumas y mul-
iplicaciones sucesivas. Fijando el alfabeto

$$x_0,\ x_1,\ x_2,\ x_3,\ldots$$

olocamos la siguiente enumeración de los polinomios (usan
o las funciones apareadoras):

$$P_1 = 1$$

$$P_{2i-1} = x_{i-1}$$

$$P_{3i} = P_{L(i)} + P_{R(i)}$$

$$P_{3i+} \quad P_{L(i)} P_{R(i)}$$

Escribimos

$$P_i = P_i(x_0, x_1, \ldots, x_n)$$

donde n es suficientemente grande como para que todas las variables que aparecen en P_i estén incluídas. (Por supuesto, en general P_i no depende de todas estas variables).

Finalmente, sea

$$D_n = \{x_0 : (\exists x_1, \ldots, x_n)[P_{L(n)}(x_0, \ldots, x_n) = P_{R(n)}(x_0, \ldots, x_n)]\} .$$

En $P_{L(n)}$ y $P_{R(n)}$ no aparecen todas las variables $x_0, \ldots, x_n$ pero claramente tampoco aparecen otras diferentes de éstas. Por la forma en que fue construída la sucesión P_i, se ve que la sucesión de conjuntos

$$D_1, D_2, D_3, D_4, \ldots$$

incluye todos los conjuntos diofantinos de enteros positivos. Todavía más:

Teorema 6.6.1. (Teorema Universal) $\{(n,x) : x \in D_n\}$ es diofantino.

Demostración.

$$x \in D_n \iff (\exists u)\{S(1,u) = 1 \wedge S(2,u) = x \wedge$$

$$\wedge(\forall i)_{\leq n}[S(3i,u) = S(L(i),u) + S(R(i),u)]$$

$$\wedge(\forall i)_{\leq n}[S(3i+1,u) = S(L(i),u)S(R(i),u)]$$

$$S(L(n),u) = S(R(n),u)\}$$

Es claro que el lado derecho de la equivalencia es diofantino. Por lo tanto, solo probaremos:

Sea $x \in D_n$ para n, x dadas. Entonces existen números $t_1,\ldots,t_n$ tales que

$$P_{L(n)}(x,t_1,\ldots,t_n) = P_{R(n)}(x,t_1,\ldots,t_n)$$

Elegimos u (por el Teorema de la Sucesión de Números) tal que:

(*) $$S(j,u) = P_j(x,t_1,\ldots,t_n) \qquad j = 1,\ldots,3n+2$$

Entonces en particular

$$S(2,u) = x$$

y

$$S(3i-1,u) = t_{i-1} \qquad i = 2,3,\ldots,n+1$$

Así, claramente el lado derecho de la equivalencia -

es verdadero. Inversamente, supongamos que para n, x dadas el lado derecho se cumple. Pongamos

$$t_1 = S(5,u),\ S(8,u) = t_2,\ldots,\ t_n = S(3n + 2,\ u)$$

Entonces (*) es cierta. Ya que

$$S(L(n),u) = S(R(n),u)$$

tenemos que

$$P_{L(n)}(x,t_1,..,t_n) = P_{R(n)}(x,t_1,\ldots,t_n)$$

Por lo tanto $x \in Dn$.

Como D_1, D_2, D_3,... nos da una enumeración de los conjuntos diofantinos, es fácil construír un conjunto diferente de todos ellos y por lo tanto no diofantino. Sea

$$\vee = \{n : n \notin D_n\}$$

<u>Teorema 6.6.2</u>. $\vee$ no es diofantino.

<u>Demostración</u>. Si $\vee$ fuera diofantino, entonces para alguna i, $\vee = D_i$. Pero tomando $i \in \vee$, tenemos:

$$i \in \vee \iff i \in D_i \quad \text{y} \quad i \in \vee \iff i \notin D_i$$

Esto es una contradicción.

<u>Teorema 6.6.3</u>. La función $g(n,x)$ definida por:

$$g(n,x) = 1 \quad \text{si} \quad x \notin D_n$$

$$g(n,x) = 2 \quad \text{si} \quad x \in D_n$$

no es recursiva.

Demostración. Si g fuera recursiva entonces g sería diofantina, *i.e.*,

$$y = g(n,x) \iff (\exists y_1,\ldots,y_m)[P(n,x,y,y_1,\ldots,y_m) = 0]$$

Así que el conjunto

$$B = \{(n,x,y) : y = g(n,x)\}$$

sería diofantino. Vamos a fijarnos en un subconjunto de B:

$$\{(x,x,y) : x \notin D_x\} = \{(x,x,1) : x \notin D_x\}$$

Entonces tenemos que:

$$= \{x : (\exists y_1,\ldots,y_m)[P(x,x,1,y_1,\ldots,y_m) = 0]\}$$

la cual contradice el Teorema 6.6.2.

Usando el Teorema 6.6.2 tenemos que

$$x \in D_n \iff (\exists z_1,\ldots,z_k)[P(n,x,z_1,\ldots,z_k) = 0]$$

donde P es algún polinomio definido (aunque complicado).

Supóngase que existiera un algoritmo para determinar si las ecuaciones diofantinas poseen soluciones enteras

positivas, *i.e.*, un algoritmo para El Décimo Problema de Hilbert. Entonces para n, x dados, este algoritmo podría usarse para determinar si la ecuación

$$P(n, x, z_1, \ldots, z_n) = 0$$

tiene o no una solución, *i.e.*, si o no $x \in D_n$. Así el algoritmo podría ser usado para calcular la función $g(n,x)$. Ya que, las funciones recursivas, justamente son aquellas para los cuales existe un algoritmo, g sería recursiva. - Esto contradice el Teorema 6.6.3 y esta contradicción prueba:

Teorema 6.6.4. El Décimo Problema de Hilbert es irresoluble.

Naturlamente este resultado no da información acerca de la existencia de soluciones para cualquier ecuación diofantina específica; este resultado, meramente garantiza - que no existe algoritmo para examinar la clase de todas - las funciones diofantina

Note que:

$$x \in \vee \iff \sim (\exists z_1, \ldots, z_k)[P(x, z_1, z_2, z_3, \ldots, z_k) = 0]$$

$$\iff \{(\exists z_1, \ldots, z_k)[P(x, z_1, \ldots, z_k) = 0 \Rightarrow 1 = 0]\}$$

$$\iff (\forall z_1, \ldots, z_k)[P(x, z_1, \ldots, z_k) > 0 \vee$$

CAPITULO II

MORTALIDAD DE CONJUNTOS DE MATRICES

1. INTRODUCCION

Sea $\phi \neq H = \{$ matrices no-nulas $n \times n$ sobre $\mathbb{C}\}$, finito.

Definición 1.1. H es mortal si existe $\{A_1, \ldots, A_k\} \subset H$ tal que $A_1 \ldots A_k = 0$

El problema referente a mortalidad de matrices dice lo siguiente:

Encontrar un algoritmo, el cual, dado H, determine si H es mortal o no.

Por ejemplo, si $n = 1$, existe un algoritmo que nos determina que H nunca es mortal.

Definición 1.2. Una palabra sobre a, b es un renglón de a's y b's tal como $baabab$. Puede ser nula.

Por ejemplo si g_1, g_2, g_3 representan las palabras bab, aa, b respectivamente, la palabra $g_2\, g_1\, g_1\, g_3$ sobre g_1, g_2, g_3 representarará la palabra $aababbabb$ sobre a, b.

Problema de Correspondencia de Post:

Determinar para un conjunto finito arbitrario (g_1, g'_1), $(g_2, g'_2), \ldots, (g_u, g'_u)$ de pares de palabras correspondientes no nulas sobre a, b, si existe una solución en n, $i_1, \ldots, i_n$ de la ecuación

$$g_{i_1} g_{i_2} \ldots g_{i_n} = g'_{i_1} g'_{i_2} \ldots g'_{i_n} \tag{2}$$

Por ejemplo, si u = 3 y

$$\{(g_1, g'_1), (g_2, g'_2), (g_3, g'_3)\} = \{(bb, b), (ab, ba), (b, bb)\}$$

Tenemos

$$g_1 g_2 g_2 g_3 = bbabbabb = g'_1 g'_2 g'_2 g'_3$$

Pero por ejemplo, si cada g_i tiene longitud mayor que la correspondiente g'_i o cada g_i empieza con una letra diferente de g'_i, la ecuación no tiene solución.

Definición 1.3. Un Sistema Normal S sobre a, b está dado por una base que consiste de una palabra inicial no nula A y un conjunto finito de operaciones: "α_i P produce Pα'_i", i = 1,..., ν donde las α'_i s y las α'_i's son palabras dadas sobre a, b y la P llamada la variable operacional representa

una palabra arbitraria sobre a , b, posiblemente nula.

Los enunciados (afirmaciones) de **S** son: **A** y todas las palabras obtenibles de **A** usando repetidamente las ν operaciones.

El problema de decisión para la clase de sistemas normales sobre a,b dice lo siguiente:

Determinar para **S** arbitrario y **B** palabra arbitraria, si **B** es un enunciado de **S**.

En este capítulo se prueba que el problema de mortalidad de matrices para $n = 3$ es irresoluble, de la siguiente forma:

En el parágrafo 2 damos la demostración debida a Michael S. Paterson de que el Problema de Mortalidad de Matrices es equivalente al Problema de Correspondencia de Post.

En el parágrafo 3 mostramos la reducción del Problema de Correspondencia de Post al Problema de Decisión para la Clase de Sistemas Normales sobre a , b.

Este último problema es recursivamente irresoluble* y por lo tanto irresoluble en el sentido intuitivo. La demos

* Es suficiente considerar "irresolubilidad recursiva" que significa - irresolubilidad en el sentido de Church [10] . Para una prueba informal de que dicho problema es recursivamente irresoluble ver [9]

tración de esta afirmación no la damos aquí en la tesis.

El método usado para $n = 3$ vale también para $n > 3$. - Por lo tanto el único caso no resuelto es para $n = 2$. Este caso lo tratamos en el parágrafo 4.

2. EL PROBLEMA DE MORTALIDAD DE MATRICES ES EQUIVALENTE AL PROBLEMA DE CORRESPONDENCIA DE POST.

Teorema 2.1. El Problema de Mortalidad de Matrices - 3 x 3 sobre los enteros es equivalente al Problema de Correspondencia de Post.

Demostración. Consideremos un conjunto H de matrices 3 x 3 sobre los enteros que consiste de las siguientes matrices:

$$S = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad , \quad T = \begin{bmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \text{ y}$$

$$W_J = \begin{bmatrix} p_J & 0 & 0 \\ 0 & r_J & 0 \\ q_J & s_J & 1 \end{bmatrix} \quad \text{donde } p_J > q_J \geq 0,\ r_J > s_J \geq 0 \text{ y } J = 1, \ldots, m.$$

Ya que

$$(a\ b\ c)\ S = a\ (1\ 0\ 1)$$

$$(a\ b\ c)\ T = (a - b)\ (1\ -1\ 0)$$

y todas las W'_J s son no sigulares, tenemos: un producto de H es cero si y solo si existe un producto X de las W'_J s tal que para algunas h, k se cumple

a) (1 -1 0) X = (0 h k)

o b) (1 -1 0) X = (h h k)

o c) (1 0 1) X = (0 h k)

o d) (1 0 1) X = (h h k)

Supongamos que se cumple a). Entonces tenemos

(a b c) T X S = 0

Supongamos que se cumple b). Entonces tenemos

(a b c) T X T = 0

Supongamos que se cumple c). Entonces tenemos

(a b c) S X S = 0

Supongamos que se cumple d). Entonces tenemos

(a b c) S X T = 0

Inversamente, es cierta la implicación ya que:

$$H_1 H_2 \cdots H_r = 0 \Rightarrow$$

$H_r = S$ ó $H_r = T$ es decir,

$(a\ b\ c)\ H_1 H_2 \cdots H_{r-1} = (o\ h\ k)$ ó $(a\ b\ c)\ H_1 \cdots H_{r-1} =$ $= (h, h, k)$ para algunas h, k; y tomando en cuenta que H_{r-1} es una W_J. Sin embargo, si

$(u_1\ u_2\ u_3)\ W_J = (v_1\ v_2\ v_3)$ para alguna J, entonces

i) $\{u_1 > 0,\ u_2 < 0$ y $u_3 = 0\} \Rightarrow \{v_1 > 0,\ v_2 < 0$ y $v_3 = 0\}$

ii) $\{u_1 > 0,\ u_2 \geq 0$ y $u_3 = 1\} \Rightarrow \{v_1 > 0,\ v_2 \geq 0$ y $v_3 = 1\}$

Para alguna J, por i)

$(1\ -1\ 0)\ W_J = (v_1\ v_2\ 0)$ donde $v_1 > 0$, $v_2 < 0$ y por lo tanto

$(1\ -1\ 0)\ X = (z_1\ z_2\ 0)$ donde $z_1 > 0$, $z_2 < 0$ de donde a) y b) son imposibles. También, por ii), para alguna J,

$(1, 0\ 1)\ W_J = (v_1\ v_2\ 1)$ con $v_1 > 0$, $v_2 \geq 0$ y por lo tanto

(1 0 1) X = (z_1 z_2 1) donde $z_1 > 0$, $z_2 \geq 0$ de donde - c) es imposible y solo d) puede cumplirse. Llegamos a:

El conjunto H es mortal si y solo si existe un producto X de las W_j's tal que

$$(1\ 0\ 1)\ X = (h\ h\ 1) \text{ para alguna } h>0$$

Dadas un par de palabras g, g' sobre el alfabeto -- {1, 2, 3} definimos la matriz

$$W(g,g') = \begin{bmatrix} p & 0 & 0 \\ 0 & \lambda & 0 \\ q & \delta & 1 \end{bmatrix}$$

donde q, δ son los números g, g' respectivamente (o 0 para la palabra nula) y p,λ son los enteros obtenidos escribiendo el uno seguido de tantos ceros como el número de símbolos en g , g' respectivamente. Por ejemplo si

$$(g,\ g') = (12132,112231233)$$

entonces

$$W\ (12132,112231233) = \begin{bmatrix} 10^5 & 0 & 0 \\ 0 & 10^9 & 0 \\ 12132 & 112231233 & 1 \end{bmatrix}$$

Las $W(g, g')$'s satisfacen las condiciones impuestos para las W_J's en H.

Si

h, h', g, g' son palabras sobre $\{1,2,3\}$

Entonces

$$(h\ h'1)W(g, g') = (hg\ h'g'\ 1)$$

Sea

$$K = \{(g_1, g_1'), (g_2, g_2'), \ldots, (g_n, g_n')\}$$

un conjunto de pares de palabras sobre $\{2,3\}$. Definimos

$$H(K) = \{S, T, W(g_J, g_J'), W(g_J, 1\ g_J'); J=1, \ldots, n\}$$

$H(K)$ es mortal si y solo si existe un producto X de las W's de $H(K)$ tal que

$$(1\ 0\ 1)\ X = (h\ h\ 1) \quad \text{para alguna } h > 0$$

Esta h tiene por primer dígito al 1 y le siguen solamente 2's y 3's. Este producto X existe si y solo si el Problema de Correspondencia para K tiene una respuesta afirmativa.

3. REDUCCION DEL PROBLEMA DE CORRESPONDENCIA DE POST AL PROBLEMA DE DECISION PARA SISTEMAS NORMALES.

Sea S un sistema normal sobre a,b cuya base consiste de la palabra inicial A y el conjunto finito de operaciones " α_i P produce P'_{α_1} " , i = 1,... ν.

Sea C y D palabras sobre a, b.

Definición 3.1. "C produce D"si y solo si para alguna P, posiblemente nula, $C = \alpha_i P$ y $D = P\alpha'_i$.

Entonces tenemos que: B es un enunciado de S si y solo si el siguiente conjunto de ecuaciones tiene solución - $i_1,\ldots, i_n$:

$$A = \alpha_{i_1} P_1, \quad P_1 \alpha'_{i_1} = \alpha_{i_2} P_2, \quad P_2 \alpha'_{i_2} = \alpha_{i_3} P_3,\ldots,$$

(2)

$$P_{n-1} \alpha'_{i_{n-1}} = \alpha_{i_n} P_n, \quad P_n \alpha'_{i_n} = B$$

Dado (2) tenemos

$$AP_1 \alpha'_{i_1} P_2 \alpha'_{i_2} \ldots P_{n-1}\alpha'_{i_{n-1}} P_n \alpha'_{i_n} = \alpha_{i_1} P_1 \alpha_{i_2} P_2 \ldots \alpha_{i_n} P_n B$$

Podemos eliminar las P's

$$(3) \qquad A\,\alpha'_{i_1}\,\alpha'_{i_2}\ldots\alpha'_{i_n} = \alpha_{i_1}\,\alpha_{i_2}\ldots\alpha_{i_n}\,B$$

Análogamente

$$(4) \qquad A\alpha'_{i_1}\,\alpha'_{i_2}\ldots\alpha'_{i_{m-1}} = \alpha_{i_1}\,\alpha_{i_2}\ldots\alpha_{i_m}P_m,\ m=1,\ldots,n$$

de donde

$$(5) \qquad \text{long}\,(A\alpha'_{i_1}\ldots\alpha'_{i_{m-1}}) \geq \text{long}\,(\alpha_{i_1}\ldots\alpha_{i_m})$$

Inversamente, dado (3) satisfaciendo (5), tenemos: $\alpha_{i_1}\ldots\alpha_{i_m}$ es igual a un"segmento inicial" de

$$A\alpha'_{i_1}\ldots\alpha'_{i_{n-1}},$$

esto ímplica que podemos determinar P_m y tener (4). Para m = 1, de (4) obtenemos la primera ecuación de (2). Sustituyendo el lado izquierdo de (4) con m = J por el derecho, tenemos para m = J + 1

$$\alpha_{i_1}\ldots\alpha_{i_J}P_J\,\alpha'_{i_J} = \alpha_{i_1}\ldots\alpha_{i_J}\alpha_{i_{J+1}}P_{J+1}$$

esto es

$$P_J\,\alpha'_{i_J} = \alpha_{i_{J+1}}P_{J+1}$$

Con esto tenemos de la segunda a la n - ésima ecuación de (2). Por último la n+ 1-ésima ecuación de (2) se obtiene de (3) vía (4) para m = n.

Se aquí que (2) tiene una solución si y solo si (3) tiene una solución que satisface (5). Es decir, B es un enuncuado de S si y solo si (3) tiene una solución en - n, $i_1,\ldots, i_n$ satisfaciendo (5). Ahora, para eliminar (5) vamos a reducir S en 3 etapas a un sistema normal en el cual (3) implique (5).

Si $C = x_1 x_2 \ldots x_n$ donde las x's son a's ó b's, sea $\bar{C} = x_n x_{n-1} \ldots x_2 x_1$. Para el sistema normal S con palabra inicial A y operaciones "α_i P produce $P\alpha_i'$" formamos el sistema S' con palabra inicial A y operaciones

$$\text{"P } \bar{\alpha}_i \text{ produce } \bar{\alpha}_i' \text{ P"}, i = 1,\ldots \nu$$

Claramente, $\bar{B}$ es un enunciado de S' si y solo si B es un enunciado de S . En seguida formamos S" con palabra inicial $\bar{A}h$ y operaciones

"P $\bar{\alpha}_i h$ produce $\bar{\alpha}'_i$ Ph", i=1,...ν

La palabra $\bar{B}$ es un enunciado de S' cuando y solamente cuando la palabra $\bar{B}h$ es un enunciado de S" . Finalmente formamos el sistema normal S"' sobre las letras a, b, h cuyos enunciados son los enunciados de S" y todas las permutaciones cíclicas de éllos. Una permutación cíclica de la palabra $x_1 \ldots x_J\ x_{J+1} \ldots x_n$ es cualquier palabra $x_{J+1} \ldots x_n\ x_1 \ldots x_J$. La palabra inicial de S"' es $\bar{A}h$. Sus $\nu + 3$ operaciones son:

"$\bar{\alpha}_i\ h$P produce P$h\ \bar{\alpha}'_i$", i=1,...ν;"aP produce Pa";

"b P produce Pb"; "hP produce Ph".

Estas tres últimas sirven para transformar una palabra sobre a, b, h en cualquiera de sus permutaciones cíclicas. Se tiene que: B es un enunciado de S si y solo si $\bar{B}h$ es un enunciado de S"'. Resimbolizamos las operaciones de S"' por:

"β_i P produce P β'_i'", i=1,...ν+3

Como S"' es un sistema normal sobre a, b, h, son válidas las ecuaciones (2) - (5). Por lo tanto, B es un enunciado de S si y solo si la siguiente ecuación (6) tiene solución que satisface (7):

(6) $$\bar{A}h\ \beta'_{i_1}\beta'_{i_2}\ldots\beta'_{i_m} = \beta_{i_1}\ldots\beta_{i_m}\bar{B}h$$

(7) $$\text{long}\ (\bar{A}h\ \beta'_{i_1}\ldots\beta_{i_{m-1}}) \geq \text{long}\ (\beta_{i_1}\ldots\beta_{i_m}),\ m=1,\ldots,n$$

Supongamos que (6) tiene una solución y para alguna m, (7) no se cumple. Para esta m

$$\text{long}\ (\beta_{i_1}\ldots\beta_{i_m}) > \text{long}\ (\bar{A}h\ \beta'_{i_1}\ldots\beta'_{i_{m-1}})$$

y por (6), tenemos

(8) $$\bar{A}h\ \beta'_{i_1}\ldots\beta'_{i_{m-1}}Q = \beta_{i_1}\ldots\beta_{i_m}$$

con Q no nula. Recordamos que

$$(\beta_i,\ \beta'_i) = (\bar{\alpha}_i\ h,\ h\bar{\alpha}'_i) \quad \text{para} \quad i = 1,\ldots,\nu$$

$$(\beta_{\nu+1},\ \beta'_{\nu+1}) = (a,\ a)$$

$$(\beta_{\nu+2},\ \beta'_{\nu+2}) = (b,\ b)$$

$$(\beta_{\nu+3},\ \beta'_{\nu+3}) = (h,\ h)$$

Como las α's y las α''s son palabras sobre $\{a, b\}$, las β_i' s y las β_i''s carecen de h o tienen exactamente una h cada una. Si la β_{i_m} de (8) fueran a's ó b's entonces el lado izquierdo de (8) tendría una h mas que el lado derecho (contradicción). El cualquier otro caso, β_{i_m} termina con h pero como **Q** es no nula, termina con h y nuevamente el lado izquierdo de (8) tiene al menos una h mas que el lado derecho. De aquí que cada solución de (6) satisface (7). Esto es; **B** es un enunciado de **S** si y solo si (6) tiene una solución.

Ahora vamos a eliminar $\bar{A}h$ y $\bar{B}h$. Introducimos $\nu + 5$ pares de palabras sobre a, b, h y k (γ_i, γ_i') correspondientes a los $\nu + 3$ pares (β_i, β_i') y a $\bar{A}h$ y $\bar{B}h$ de la siguiente manera:

Las x's y y's representan a's, b's ó h's

Si

$$(\beta_i, \beta_i') = (x_1 \cdots x_k, y_1 \cdots y_\lambda)$$

Entonces

$$(\gamma_i, \gamma_i') = (x_1 k\ x_2 k \cdots x_k k, k y_1\ k y_2 \cdots k y_\lambda),\ i=1, \ldots \nu + 3.$$

Si

$$(\bar{A}h\ ,\ \bar{B}h) = (y_1 \cdots y_\lambda,\ x_1 \cdots x_k)$$

Entonces

$$(\gamma_{\nu+4}, \gamma'_{\nu+4}) = (kk,\ kky_1 ky_2 \ldots ky_\lambda)$$

$$(\gamma_{\nu+5},\ \gamma'_{\nu+5}) = (x_1 kx_2 k \ldots x_k kk,\ kk)$$

Afirmamos que

$$\bar{A}h\ \beta'_{i_1} \ldots \beta'_{i_n} = \beta_{i_1} \ldots \beta_{i_n}\ \bar{B}h$$

tiene una solución en n, $i_1,\ldots,i_n$, $n \geq 0, i_p = 1,\ldots,\nu+3$ si y solo si

(9) $$\gamma'_{J_1}\ \gamma'_{J_2} \ldots \gamma'_{J_m} = \gamma_{J_1}\ \gamma_{J_2} \ldots \gamma_{J_m}$$

tiene una solución en m, $J_1,\ldots,J_m$, $m \geq 1$,

$J_q = 1,\ldots,\ \nu + 5$

Supongamos que existen $i_1,\ldots,i_n$ tales que

$$\bar{A}h\ \beta'_{i_1} \ldots \beta'_{i_n} = z_1 z_2 \ldots z_l = \beta_{i_1} \ldots \beta_{i_n}\ \bar{B}h$$

entonces

$$(J_1,\ldots,J_m)=(\nu+4,i_1,\ldots,i_n,\nu+5)$$

hace a (9)

$$\gamma'_{\nu+4}\ \gamma'_{i_1}\cdots\gamma'_{i_n}\gamma_{\nu+5}=kkz_1kz_2kz_3\cdots kz_1kk=\gamma_{\nu+4}\gamma_{i_1}\cdots\gamma_{\nu+5}$$

Ahora supongamos que existen $J_1,\ldots,J_m$ tal que

$$\gamma'_{J_1}\cdots\gamma'_{J_m}=\gamma_{J_1}\cdots\gamma_{J_m}$$

Entonces, como γ'_{J_1} y γ_{J_1} deben empezar con la misma letra, tenemos que $J_1=\nu+4$. Análogamente $J_m=\nu+5$ pues γ_{J_m} y γ'_{J_m} deben terminar con la misma letra. Si todas las J's intermedias son diferentes de $\nu+4$ y $\nu+5$ éstas dan directamente una sucesión de i's las cuales satisfacen (6). En cualquier otro caso, sea J_u la primer J después de J_1 que es $\nu+4$ ó $\nu+5$. Si $J_u=\nu+4$, tenemos

$$\gamma'_{J_1}\ \gamma'_{J_2}\cdots\gamma'_{J_u}=kkx_1kx_2\ldots kx_pkkx_{p+1}kx_{p+2}\ldots kx_q$$

$$\gamma_{J_1}\ \gamma_{J_2}\cdots\gamma_{J_u}=kky_1ky_2\ldots ky_rkkk$$

Las x's y las y's son a's, b's ó h's. La segunda vez que aparece kk en $\gamma'_{J_1} \ldots \gamma'_{J_u}$ está seguida por a, b ó h y en $\gamma_{J_1} \ldots \gamma_{J_u}$ está seguida por k. Esto contradice (9). De aquí que $J_u = \nu + 5$ y por lo tanto

$$\gamma'_{J_1} \ldots \gamma'_{J_u} = kkx_1 kx_2 \ldots kx_p kk$$

$$\gamma_{J_1} \ldots \gamma_{J_u} = kky_1 ky_2 \ldots ky_q kk$$

Pero como, antes de que aparezca por segunda vez kk, los lados izquierdo y derecho de (9) deben ser iguales, tenemos

$$\gamma'_{J_1} \ldots \gamma'_{J_u} = \gamma_{J_1} \ldots \gamma_{J_u}$$

y así, tenemos una solución de (9) de la forma vista anteriormente y que por lo tanto nos lleva a una solución de (6).

De aquí se sigue que:

B es un enunciado de **S** si y solo si (9) tiene una solución.

En la reducción efectuada introdujimos las nuevas letras h y k. Pero vamos ahora a reemplazar las letras a, b,

h y k por bab, $baab$, $baaab$ y $baaaab$ respectivamente. Llamamos a los pares resultantes de palabras sobre a, b, (δ_i, δ'_i). Entonces (9) es equivalente a

$$\delta'_{J_1}\ \delta'_{J_2} \ldots \delta'_{J_m} = \delta_{J_1}\ \delta_{J_2} \ldots \delta_{J_m} \tag{10}$$

Dados un sistema normal S sobre a, b con palabra inicial A, operaciones: "α_i P produce $P\alpha'_i$" y una palabra B - sobre a, b, lo expuesto anteriormente da un método para formar los pares de palabras (δ_i, δ'_i) sobre a, b, tales que:

> B es un enunciado de S si y solo si (10) tiene una - solución.

Por lo tanto, efectivamente hemos reducido el Problema de Decisión para la clase de Sistemas Normales al Problema de Correspondencia de Post. Entonces, si el primero es irresoluble también lo es el segundo. Actualmente se puede verificar (aunque aquí no lo hacemos) que la reducción efectuada es recursiva y por lo tanto la irresolubilidad recursiva del primer problema conduce a la irresolubilidad recursiva del Problema de Correspondencia.

4. MORTALIDAD DE MATRICES 2 x 2.

Como mencionamos antes el caso no resuelto es para $n = 2$. En este caso, H es un conjunto no vacío, finito, de matrices 2 x 2 sobre los complejos, distintas de cero -- ($H \subset M_2 (\mathbb{C})$)

Es fácil ver que H es mortal si y solo si algún producto

$$A_1 \; A_2 \; \ldots \; A_k = 0$$

con los rangos de A_1 y A_k iguales a 1 y los rangos de las restantes matrices $A_2, \ldots, A_{k-1}$ iguales a 2.

De derecha a izquierda la implicación es obvia.

Inversamente, supongamos que H es mortal, i.e., que - que existe $\{B_1, \ldots, B_r\} \subset H$ tal que

$$B_1 \; \ldots \; B_r = 0 \tag{1}$$

Vamos a demostrar por inducción sobre el número de matrices que podemos reducir el producto en (1) hasta la forma deseada

Para $n = 2$

Sea $B_1 B_2 = 0$. Claramente B_1 y B_2 deben ser de rango 1 pues lo contrario llevaría a que B_1 o B_2 son cero.

Para $n = 3$

Sea $B_1 B_2 B_3 = 0$. Si alguna de las matrices B_1, B_3 es de rango 2, digamos B_1, tenemos el caso anterior, es decir

$$B_2 B_3 = 0$$

Por lo tanto podemos suponer que B_1 y B_3 son de rango 1. Sean $\mathcal{R}_1$ y $\mathcal{R}_2$ los rangos de B_3 y $B_2 B_3$ respectivamente

$$\mathbb{C}^2 \xrightarrow{B_3} \mathcal{R}_1 \xrightarrow{B_2} \mathcal{R}_2 \xrightarrow{B_1} \{0\}$$

Si B_2 es de rango 1 entonces $\mathcal{R}_2 = \{0\}$ o es un subespacio de dimensión 1; en el primer caso tenemos que

$$B_2 B_3 = 0$$

y en el segundo caso

$$B_1 B_2 = 0$$

Ahora supongamos inductivamente que cualquier producto igual a cero de k-matrices podemos reducirlo a un producto igual a cero de la forma deseada.

Sea

$$B_1 \dots B_{k+1} = 0 \tag{2}$$

Si alguna de las matrices B_1, B_{k+1} es de rango 2, B_1 por ejemplo, entonces

$$B_2 \dots B_{k+1} = 0$$

y podemos aplicar la hipótesis de inducción

Supongamos entonces que B_1 y B_{k+1} son de rango 1. Si alguna B_J, $J \neq 1, k+1$ es de rango 1, entonces denotando

$$A_1 = B_1 \dots B_{J-1}\ , \quad A_2 = B_{J+1} \dots B_k$$

y $\mathcal{R}_1$, $\mathcal{R}_2$ y $\mathcal{R}_3$ los rangos de B_{k+1} , $A_2\ B_{k+1}$ y $B_J\ A_2\ B_{k+1}$ respectivamente

$$\mathbb{C} \xrightarrow{B_{k+1}} \mathcal{R}_1 \xrightarrow{A_2} \mathcal{R}_2 \xrightarrow{B_J} \mathcal{R}_3 \xrightarrow{A_1} \{0\}$$

tenemos que $\mathcal{R}_3 = \{ 0 \}$ o $\mathcal{R}_3$ es un subespacio de dimensión 1; en el primer caso se tiene que

$$B_J \, B_{J+1} \, \ldots \, B_{k+1} = 0$$

y en el segundo caso,

$$B_1 \, B_2 \, \ldots \, B_J = 0$$

En ambos casos aplicamos la hipótesis de inducción

Por lo anterior, afirmamos que el problema de mortalidad es equivalente al siguiente problema:

Encontrar un algoritmo, el cual, dado un conjunto finito H' de transformaciones lineales no singulares del plano complejo ($T : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$) y lineas L y M que pasan por el origen, determinar si existe algun producto de H' que mande L en M .

Primero supongamos que existe un algoritmo que para todo $H \subset M_2 (\mathbb{C}) - \{ 0 \}$, finito, determine si existe $\{A_1, \ldots, A_k\} \subset H$ tal que

$$A_1 \, A_2 \, \ldots \, A_k = 0$$

con A_1 y A_k de rango 1 y $A_2, \ldots, A_{k-1}$ de rango 2. Sean $H' \subset GL(2, \mathbb{C})$, finito, L y M lineas (en $\mathbb{C}^2$) que pasan por el origen, y $A \in M_2(\mathbb{C})$ tal que

$$\text{Núcleo}(A) = M \quad y \quad A(\mathbb{C}^2) = L$$

(por brevedad de notación identificamos las transformaciones lineales con sus matrices con respecto a una base fija).

Tomamos

$$H = H' \cup \{ A \}$$

Nuestra hipótesis es que existe un algoritmo que determina si existen $A_1, \ldots, A_k \in H'$ tal que

$$A A_1 \ldots A_k A = 0$$

o sea, tal que

$$A_1 \ldots A_k (L) = M$$

Inversamente, supongamos que existe un algoritmo que para todo H' y L y M como antes, determine si existe un producto $A_1 \ldots A_k$ tal que

$$A_1 A_2 \ldots A_k (L) = M$$

Sea $H \subset M_2(\mathbb{C})$, finito; mediante un número finito de pa-- sos podemos descomponer H en H_1 y H_2 donde

$$H_1 = \{A \in H : |A| \neq 0\} \text{ y } H_2 = \{A \in H : |A| = 0\}$$

Tomamos una pareja de matrices de H_2 y la denotamos por - (A_0, A_{k+1}). Llamamos L a la imagen de $\mathbb{C}^2$ bajo A_{k+1} y M al núcleo de A_0. Aplicamos el algoritmo a H_1 con L y M. Pode mos saber si existe $A_1, \ldots, A_k$ tales que

$$A_1 \ldots A_k (L) = M$$

esto es, tales que

$$A_0 A_1 \ldots A_k A_{k+1} = 0$$

para $A_0, A_{k+1} \in H_2$. Como el número de parejas ordenadas - de H_2 es finito, hacemos esto para cada pareja ordenada y - por lo tanto tenemos un algoritmo que nos dice si existe o no $\{B_1, \ldots, B_r\} \subset H$ tal que

$$B_1 B_2 \cdots B_{r-1} B_r = 0$$

con $B_1, B_r \in H_2$ y $B_2, \ldots, B_{r-1} \in H_1$

Este problema de Mortalidad puede resolverse en algunos casos especiales, por ejemplo cuando H contiene solamente matrices triangulares superiores; una solución positiva general sería de interés tanto para geómetras como para algebristas. Una solución negativa, nos daría un nuevo tipo de problema irresoluble.

CAPITULO III

CONSTRUCTIBILIDAD DE LOS NUMEROS REALES

1. INTRODUCCION

Más propiamente "cómo definir (matemáticamente hablando) el llamado sistema de los números reales". Actualmente todo estudiante de Matemáticas, en el nivel profesional debe conocer, las diversas teorías sobre el sistema de los números reales: Cortaduras de Dedekind en el campo racional, Sucesiones (infinitas) convergentes de Cauchy– Cantor de números racionales, Sucesiones (infinitas) decimales de Kroneker, "Sureal Numbers" Knudth. Todas estas construcciones de los números reales remiten a la caracterización axiomática del "sistema de los números reales" consistente en que es un campo ordenado arquimedianamente máximo y en el cual todo subconjunto acotado superiormente tiene una frontera superior (que pertenece al conjunto).

Ahora bien, en las aplicaciones de la Matemática y en esta misma se calcula y opera no generalmente con los números reales mismos sino con aproximaciones racionales (tan finas como sean necesarias) de estos y a las que llamaremos "números reales humanamente calculables", pero ello

se hace de manera imprecisa, incontrolada y desde luego - no aceptable para el rigor matemático. Esto obliga a considerar la existencia y construcción de un campo que satisfaga lo más posible los axiomas para el campo real y al - mismo tiempo que tenga elementos que se parezcan mucho a los "números reales humanamente calculables". Esto es, - para los que se puedan definir algoritmos finitos para - calcular con ellos.

Consideraremos la noción de número real desde un - punto de vista constructivo. Este punto de vista requiere que cualquier número real pueda ser calculado.

Explicaremos varios sentidos en los cuales se puede decir que un número real ha sido construído y explicaremos por qué algunos de éstos, son inapropiados para el propósito de desarrollar el análisis constructivamente.

Me interesa enfatizar que para no alargar demasiado la tesis, solo trate los que pudieran llamarse tópicos - inicales sobre este tema. Esto va en concordancia con el nivel de Licenciatura al que corresponde mi tesis.

2. NUMEROS REALES DECIMALES

Nuestro primer intento por explicar qué se entiende por un número real es el siguiente:

Definición 2.1 α es un número real si se puede dar una regla para calcular su n-ésima cifra decimal.

Así que, α lo podemos identificar con una función $\phi : \mathbb{N} \cup \{0\} \longrightarrow \mathbb{Z}$ donde ϕ (0) es la parte entera de α y para $n > 0$, ϕ (n) $\in \{0,1,\ldots,9\}$.

Denotaremos el conjunto de los números reales en el sentido de esta definición por $\mathbb{R}_d$ (d por decimal).

Aunque la mayoría de los números reales (por ejemplo los algebraicos y los trascendentes e y π) son constructibles en este sentido, demostraremos que $\mathbb{R}_d$ no es adecuado como un fundamento para el análisis.

Teorema 2.1 El conjunto $\mathbb{R}_d$ no es cerrado bajo la adición, es decir, existen números $\alpha, \beta \in \mathbb{R}_d$ tal que $\alpha + \beta \notin \mathbb{R}_d$.

Demostración. El "no" del teorema está usado en el sentido histórico; esto es, decir que una proposición no es verdadera significa que todavía no se ha probado. Daremos dos números α y β tal que cada uno de ellos se le pueda calcular cualquier número de cifras decimales mientras que todavía nadie conoce la primera cifra decimal de $\alpha + \beta$. Para demostrar esta afirmación (histórica) usare-

remos nuestra ignorancia (histórica) del comportamiento de la expansión decimal de π .

Específicamente, nadie sabe si la sucesión 5555 aparece en esta expansión. Si esta sucesión aparece por primera vez y comienza en la k-ésima cifra decimal, entonces k es llamado el número crítico (de π). No se sabe si un número tal existe y tampoco se sabe, si existe, si es par o impar. Además, dado cualquier entero n no negativo , evidentemente se puede determinar si n es un número crítico ó no; para esto basta calcular la primera $n+3$ cifras decimales de π .

Para calcular α lo hacemos de la siguiente forma:

Cualquier cifra decimal de α es 3 a menos que el número $2n+1$ sea el número crítico de π ; en este caso la $2n+1$ cifra decimal de α es 4 y las demás son 3's. Así que, si el número crítico de π, k, es impar $\alpha > \frac{1}{3}$, pero si k, es par ó no existe, entonces $\alpha = \frac{1}{3}$.

Para calcular β lo hacemos de la siguiente forma:

Cualquier cifra decimal de β es 5 a menos que el número $2n$ sea el número crítico de π; en este caso la $2n$ cifra decimal de β es 5 y las demás son 6's. Así que, si el número crítico k de π es par, $\beta < \frac{2}{3}$ pero si k es impar o no existe, entonces $\beta = \frac{2}{3}$ ("k no existe" significa que 5555 no aparece en la expansión decimal de π).

Tenemos:

$$\text{Si } k \text{ es par, } \alpha = \frac{1}{3} , \beta < \frac{2}{3} , \alpha + \beta < 1$$

$$\text{Si } k \text{ es impar, } \alpha > \frac{1}{3} , \beta = \frac{2}{3} , \alpha + \beta > 1$$

$$\text{Si } k \text{ no existe, } \alpha = \frac{1}{3} , \beta = \frac{2}{3} , \alpha + \beta = 1$$

Ahora, supongamos que escribiéramos la primera cifra decimal de $\alpha + \beta$. Entonces si $\alpha + \beta$ empieza con 1....entonces $\alpha + \beta \geq 1$ y si k existe es impar. Mientras que:

Si $\alpha + \beta$ empieza con .9... entonces $\alpha + \beta \leq 1$ y si k existe es par.

Es decir, si pudiéramos calcular la primer cifra decimal de $\alpha + \beta$, demostraríamos una de las dos proposiciones: "si k existe, es impar" o "si k existe, es par". Esto es, probaríamos: "si 5555 apareciera en π, su primera aparición empezaría en un lugar impar" o "si 5555 apareciera en π, su primera aparición empezaría en un-lugar impar". Pero no tenemos probada ninguna de estas dos proposiciones; así que no podemos escribir la primera cifra decimal de $\alpha + \beta$ y si podemos escribir todas las cifras decimale de α y de β. Esto completa la prueba del teorema 2.1.

3. NUMEROS REALES LOCALIZADOS.

Ahora consideramos otra posible aproximación a los números reales.

Definición 3.1. Un número real λ es localizado con respecto a los racionales si podemos decidir para cada racional r, cuál de las tres alternativas vale:

$$\lambda < r,\ \lambda = r,\ \lambda > r$$

Denotaremos al conjunto de los números reales localizados por $\mathbb{R}_\ell$ (ℓ por localizado).

Teorema 3.1. $\mathbb{R}_\ell \subset \mathbb{R}_d$ y $\mathbb{R}_d \not\subset \mathbb{R}_\ell$

Demostración. Primero vamos a demostrar que $\mathbb{R}_\ell \subset \mathbb{R}_d$.

Sea $\lambda \in \mathbb{R}_\ell$. Sea M un entero cota superior de $|\lambda|$.

Comparemos λ con cada uno de los enteros

$$-M, -M+1, -M+2, \ldots, 0, 1, \ldots, M-1, M$$

para encontrar la parte entera de λ, que le llamaremos q; enseguida comparamos λ con cada uno de los números

$$q + \frac{1}{10}, \quad q + \frac{2}{10}, \ldots, \quad q + \frac{9}{10}$$

para encontrar la primera cifra decimal de λ y así sucesivamente.

Para demostrar que $\mathbb{R}_d \not\subset \mathbb{R}_\ell$, debemos dar un número con expansión decimal que no sea localizado con respecto a los racionales. El número α del teorema anterior es de este tipo, ya que no podemos decidir cuál de las tres posiciones es verdadera: " $\alpha < \frac{1}{3}$," "$\alpha = \frac{1}{3}$", " $\alpha > \frac{1}{3}$ ". De aquí que $\alpha \in \mathbb{R}_d - \mathbb{R}_\ell$.

Por lo tanto la condición de ser localizado es estrictamente más fuerte que la de tener una expansión decimal. Además la mayoría de los números reales, encontrados en análisis son localizados, por ejemplo los números algebraicos y los trascendentes e y π como fue probado por Goodstein. Para ilustrar veremos que $\sqrt{2}$ es localizado. Para determinar si un racional r es menor o mayor que $\sqrt{2}$ (por supuesto que= es imposible) primero preguntamos si $r \leq 0$; sí asi es, $r < \sqrt{2}$, si no, calculamos r^2 y preguntamos si r^2 es menor a mayor que 2. Una propiedad más fuerte de $\sqrt{2}$ la probamos en el siguiente teorema:

Teorema 3.2 Para cualquier número racional r, podemos calcular un número n_r tal que:

$$|r - \sqrt{2}| > \frac{1}{10^{n_r}}$$

(esto significa que la expansión decimal de r difiere de $\sqrt{2}$ en o antes de la n_r-ésima cifra decimal).

Demostración. Tenemos:

$$|r-\sqrt{2}| \geq ||r|-\sqrt{2}| = \left|\frac{r^2-2}{|r|+\sqrt{2}}\right| = \frac{|r^2-2|}{|r|+\sqrt{2}} > \frac{|r^2-2|}{|r|+2}$$

Así que, escogemos n_r tal que

$$\frac{1}{10^{n_r}} < \frac{|r^2-2|}{|r|+2}$$

Probablemente se pensará que cualquier número "razonable" es localizado y que por lo tanto podríamos definir los "números reales humanamente calculables" como números reales localizados. Sin embargo, el teorema siguiente afirma lo contrario.

Teorema 3.3. $\mathbb{R}_\ell$ no es cerrado bajo la adición, es decir, existen números γ, $\delta \in \mathbb{R}_\ell$ tales que $\gamma+\delta \notin \mathbb{R}_\ell$.

Demostración. Sea $\gamma = -\sqrt{2}$. No sabemos si la sucesión 5555 aparece en la expansión decimal de $\sqrt{2}$.- Definimos el número crítico de $\sqrt{2}$ de la forma como definimos el número crítico de π. Para calcular δ escribimos la expansión decimal de $\sqrt{2}$ excepto si n es el número crítico de $\sqrt{2}$; en este caso la n-ésima cifra decimal de δ es 0. Antes de demostrar que $\delta \in \mathbb{R}_\ell$, demostraremos que $\gamma+\delta \notin \mathbb{R}_\ell$. Para esto demostraremos que $\gamma+\delta$ no es localizado con respecto a 0:

Si $\gamma+\delta = 0$, tenemos que $\delta = \sqrt{2}$ y esto nos dice que la proposición "5555 no aparece en la expansión decimal de $\sqrt{2}$" es verdadera.

Si $\gamma+\delta < 0$ tenemos que la proposición "5555 aparece en la expansión decimal de $\sqrt{2}$"es verdadera.

Ahora sí, probaremos que $\delta \in \mathbb{R}_\ell$; para esto veremos que para cualquiera racional r, podemos decir cuál de las tres proposiciones se cumple:

$$\delta < r \ , \ \delta = r \ , \ \delta > r$$

CASO I. $r > \sqrt{2}$.

En este caso $r > \delta$ pues $\delta \leq \sqrt{2}$.

CASO II. $r < \sqrt{2}$.

Por el teorema 3.2 podemos encontrar n tal que

$$|r - \sqrt{2}| > \frac{1}{10^n}$$

Sea n_0 la menor de las n's donde r y $\sqrt{2}$ defieren. Entonces si (Subcaso II.1) no existe número crítico de $\sqrt{2}$ menor o igual que n_0, $\sqrt{2}$ y δ coinciden para sus primeras n_0 cifras y por lo tanto $r < \delta$. En el otro caso (Subcaso II.2), si existe el número crítico y es menor o igual que n_0, podemos calcular δ y lo comparamos con r directamente. En cualquier caso podemos decidir si r es menor, igual o mayor que δ y así, $\delta \in \mathbb{R}_\ell$.

En este teorema se prueba que $\mathbb{R}_\ell$ no se puede usar como un fundamento para el análisis.

4. NUMEROS REALES DECIMALMENTE APROXIMABLES

Ahora daremos la definición de número real que termi

na con las dificultades anteriores.

Definición 4.1. Un decimal finito es un número de la forma $a/10^b$ donde a es un entero y b un entero no-negativo.

Definición 4.2. Un número real ρ es llamado decimalmente aproximable ($\rho \in \mathbb{R}_{da}$) si dado cualquier racional $\varepsilon > 0$ podemos encontrar un decimal finito d tal que

$$| \rho - d | < \varepsilon$$

Teorema 4.1 $\mathbb{R}_d \subset \mathbb{R}_{da}$ y $\mathbb{R}_{da} \not\subset \mathbb{R}_d$.

Demostración. Sea $\rho \in \mathbb{R}_d$. Entonces por definición podemos calcular cualquier número de cifras decimales de ρ, Para aproximarnos con $\frac{1}{10^n}$ solamente necesitamos calcular $n + 1$ cifras; de aquí que ρ $\mathbb{R}_{da}$. Para refutar el inverso, observemos que la suma de dos elementos de $\mathbb{R}_{da}$ está en $\mathbb{R}_{da}$. Sean ρ_1 y $\rho_2 \in \mathbb{R}_{da}$; si d_1 y d_2 son $\varepsilon/2$- aproximaciones a ρ_1 y ρ_2 respectivamente, entonces

$$|(d_1+d_2) - (\rho_1+\rho_2)| \leq |d_1-\rho_1| + |d_2-\rho_2| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

Así que d_1+d_2 es una ε-aproximación a $\rho_1+\rho_2$. Por lo tan

to $\rho_1 + \rho_2 \in \mathbb{R}_{da}$.

Ahora, sean $\alpha, \beta \in \mathbb{R}_d$ y $\alpha + \beta \notin \mathbb{R}_d$ y $\alpha+\beta \in \mathbb{R}_{da}$.

Así que, los números reales decimalmente aproximables son un candidato más aceptable que $\mathbb{R}_d$ y $\mathbb{R}_\ell$ como un fundamento para el análisis constructivo.

El siguiente teorema confirma esta impresión:

Teorema 4.2. $\mathbb{R}_{da}$ es un campo.

Demostración. ya probamos que $\mathbb{R}_{da}$ es cerrado bajo la adición; como un ejemplo de la verificación de los postulados para campo probaremos que $\mathbb{R}_{da}$ es cerrado bajo la multiplicación. Sean $\rho_1, \rho_2 \in \mathbb{R}_{da}$. Buscamos una ε- aproximación a $\rho_1 \rho_2$. Primero calculamos un número $M > \max(|\rho_1|, |\rho_2|)$. Ahora encontramos $\varepsilon/2M$-aproximaciones d_1, d_2 a ρ_1, ρ_2 respectivamente con $|d_1|, |d_2| < M$.

Tenemos

$$|d_1-\rho_1| < \varepsilon/2M$$

$$|d_2-\rho_2| < \varepsilon/2M$$

$$|d_1 d_2-\rho_1\rho_2| = |d_1(d_2-\rho_2) + \rho_2 (d_1-\rho_1)| \leq$$

$$\leq |d_1|\ |d_2-\rho_2| + |\rho_2|\ |d_1-\rho_1|$$

$$< M\,\varepsilon/2M + M\,\varepsilon/2M = \varepsilon$$

Así que, $d_1 d_2$ es una ε-aproximación a $\rho_1 \rho_2$

Para verificar los postulados de campo, tenemos que estar seguros que las afirmaciones de algunos de ellos tienen sentido constructivo. Por ejemplo, en el postulado

$$(*) \qquad x \neq 0 \Rightarrow (\exists y)\ (x\,y = 1)$$

debemos ser cuidadosos para dar el significado correcto a la hipótesis $x \neq 0$ ya que es fácil construír un número el cual no es menor, igual o mayor que cero. Por ejemplo, el número $\gamma+\delta$ en el teorema 3.3, es de este tipo. Tenemos que $x=\gamma+\delta \in \mathbb{R}_{da}$ pero x no es $<,=o>$ cero. ¿Cómo construímos (*) para esta x?. La versión correcta es:

Si x está separado de cero, i.e., si conocemos un racional r tal que $0 < r < |x|$, entonces x posee un recíproco.

Esta noción de separación es un ejemplo de como las matemáticas constructivas (excepto en contraejemplos) normalmente reemplaza afirmaciones negativas por positivas.

A algunos lectores les puede sorprender que $\mathbb{R}_{da}$ es un campo completo, en el sentido de que si $\{\rho_i\}$ es una sucesión de elementos de $\mathbb{R}_{da}$ tal que para cada $\varepsilon > 0$ podemos calcular N_ε tal que

$$|\rho_i - \rho_j| < \varepsilon \quad (i, j > N_\varepsilon$$

entonces podemos construír un número $\rho \in \mathbb{R}_{da}$ que satisface:

$$(\forall \varepsilon)\ (\exists M_\varepsilon)\ (\forall i > M_\varepsilon)\ |\rho_i - \rho| < \varepsilon$$

De hecho, la prueba es un cálculo directo con ε's y δ's.

Por supuesto, $\mathbb{R}_{da}$ no es un campo ordenado. Ya conocemos un ejemplo de un elemento $x = \gamma + \delta$ de $\mathbb{R}_{da}$ el cual no es ni mayor que cero, ni menor que cero, ni igual a cero.

Concluímos tratando de precisar la diferencia entre análisis constructivo y análisis recursivo. Lo que hemos estado haciendo en este capítulo es análisis constructivo.

Aquí no se permiten números reales que no sean computables ni métodos de prueba que no sean constructivos y el concepto de "función computable" o "regla" es un concepto primitivo. Por otro lado, el análisis recursivo, es el estudio, de un cierto subconjunto de los números reales, clásicamente definido, llamado los reales recursivos*. "Computable" es simplemente un sinónimo de "recursivo" y es una idea definida. Desde el punto de vista de lo que llamamos análisis recursivo, los conjuntos $\mathbb{R}_d$, $\mathbb{R}_\ell$ y $\mathbb{R}_{da}$ son el mismo conjunto pero la prueba de que ellos son el mismo no es constructiva.

*$\alpha = A.\ \alpha_1\ \alpha_2\ \alpha_3\ \ldots$ es un real recursivo si la función $f(i) = \alpha_1$ es recursiva.

REFERENCIAS

1. Martín Davis, *Hilbert's Tenth Problem is Unsolvable*, The American Mathematical Monthly, Vol.80 (1973) - 233-269.

2. Martín Davis and Reuben Hersch, *Hilbert's Tenth - Problem*, Scientific American, Noviembre (1973) 84-91.

3. Julia Robinson, *Diophantine decisión problems*, MMA Studies in Mathematics, 6 (1969) [Studies in Number theory, edited by W.J. Le Veque, 76-116].

4. B.A. Trajtenbrot, *Los Algoritmos y la Resolución Automática de Problemas*, Editorial Mir, Moscú.

5. William J. Le Veque, *Fundamentals of Number Theory*, Addison Wesley, 1977, Capítulo 2.

6. P. Schultz, *Mortality of 2X2 matrices*, The American Mathematical Monthly, (1977) 463-464.

7. M.S. Paterson, *Unsolrability in 3X3 matrices*, Studies in Applied Mathematics, 49 (1970) 105-107

8. E.L. Post, *A variant of a recursively unsolvable - problem*, Bulletín of the American Mathematical - Society, 52 (1946) 264-268.

9. E.L. Post, *Recursively enumerable sets of positive integers and their decision problems*, Bull. Amer. - Math. Soc. Vol.50 (1944) 284-316.

10. Alonso Church, *An unsolvable problem of elementary number theory*, Amer. J.Math. Vol.58 (1936) 345-363.

11. John Myhill, *what is a Real Number?*, The American - Mathematical Monthly, Vol.79 (1972) 748-754.