UNIVERSIDAD NACIONAL DE LA MATANZA

ESCUELA DE FORMACIÓN CONTINUA

LICENCIATURA EN MATEMÁTICA APLICADA

TRABAJO FINAL DE TESIS

“EL DÉCIMO PROBLEMA DE HILBERT”

Autora: Francese, Silvina A.

Profesor: Lic. Miguel Calzón

Año de cursada 2010

ÍNDICE

Introducción……..3

Conjuntos diofánticos……..4

La ecuación de Pell……...5

Funciones diofánticas……..16

Conjuntos y funciones recursivas……..20

Máquina de Turing y la tesis de Church-Turing……28

Teorema de Matijasevic y solución al décimo problema de Hilbert……...32

Conclusión……37

Bibliografía……..38

Introducción

"¿Quién de nosotros no quisiera levantar el velo tras el cual yace escondido el futuro, y asomarse, aunque fuera por un instante, a los próximos avances de nuestra ciencia y a los secretos de su desarrollo ulterior en los siglos futuros? ¿Cuáles serán las metas particulares que tratarán de alcanzar los líderes del pensamiento matemático de las generaciones futuras? ¿Qué nuevos métodos y nuevos hechos nos depararán los siglos por venir en el ancho y rico campo del pensamiento matemático?"

Con estas palabras comenzó David Hilbert su discurso en el Primer Congreso Internacional de Matemáticas, celebrado en París, donde fue uno de los principales conferenciantes. Esperando orientar a los matemáticos de la época de forma similar, Hilbert presentó un conjunto de 23 problemas no resueltos en matemáticas. Algunos de ellos permanecen hoy sin resolver, otros han sido reformulados y, tal vez lo más importante, todos ellos han inspirado a los matemáticos durante 100 años.

En este trabajo desarrollaremos el décimo problema el cual se pregunta acerca de la existencia de un algoritmo general para decidir sobre la solubilidad de ecuaciones diofánticas. Usando los trabajos de Matin Davis, Hilary Putnam y Julia Robinson, Yuri Matijasevic en 1970 respondió negativamente a esta cuestión. El teorema que plantea Matijasevic implica la no existencia de un algoritmo para el décimo problema de Hilbert.

Formalmente el décimo problema de Hilbert enuncia lo siguiente:

Determinación de la solubilidad de ecuaciones diofánticas. *Dada una ecuación diofántica con un número de incógnitas arbitrario y con coeficientes enteros: encontrar un procedimiento mecánico, que en un número finito de pasos, determine si una ecuación diofántica tiene solución en los enteros.*

Hilbert estaba interesado en una solución positiva al problema. Si bien hay muchas técnicas para resolver muchos tipos de ecuaciones diofánticas, veremos que algunas no pueden ser decididas por método alguno.

El propósito del presente trabajo es dar una prueba de la insolubilidad del décimo problema de Hilbert. Para el cual se utilizó sólo una parte del trabajo realizado por Matijasevic, dejando aún lado los lenguajes de programación, enfocando en el desarrollo teórico del mismo.

§1 Conjuntos Diofánticos

Una ecuación diofántica es una ecuación polinómica $P(a_1, \dots, a_m, x_1, \dots, x_n) = 0$ en varias variables, con coeficientes enteros. Las variables se dividen en los parámetros $a_1, \dots, a_m$ e incógnitas $x_1, \dots, x_n$. Todas las variables, parámetros e incógnitas pertenecen al conjunto de los números enteros no negativos: 0, 1, 2,…

En la teoría clásica de ecuaciones diofánticas uno comienza con una ecuación y busca los valores de los parámetros para los cuales existe una solución. En esta prueba cambiamos el procedimiento generalmente. Comenzamos con la solución y buscamos la ecuación que se verifique esta solución. Comenzamos con una relación $A(a_1, \dots, a_m)$ y buscamos un polinomio $P(a_1, \dots, a_m, x_1, \dots, x_n)$ definido como en (1).

Definición 1.1: Una relación o conjunto $A(a_1, \dots, a_m)$ es **diofántica** si existe un polinomio $P(a_1, \dots, a_m, x_1, \dots, x_n)$ tal que para todos los valores de $a_1, \dots, a_m$, (los parámetros)

$$A(a_1, \dots, a_m) \Leftrightarrow (\exists x_1, \dots, x_n)[P(a_1, \dots, a_m, x_1, \dots, x_n) = 0]$$

Esta definición la cuál es para relaciones, también se aplicará a funciones. Una función se dirá que es diofántica si su representación es diofántica.

Definición 1.2: La función $f: N^n \rightarrow N$ es diofántica si existe una ecuación diofántica $D(a, a_1, \dots, a_m, x_1, \dots, x_n) = 0$ tal que

$$y = f(a_1, \dots, a_m) \Leftrightarrow \exists x_1, \dots, x_n D(y, a_1, \dots, a_m, x_1, \dots, x_n) = 0$$

Ejemplos:

$$a \leq b \Leftrightarrow (\exists x)[a + x = b] \qquad (1.3)$$

$$a|b \Leftrightarrow (\exists x)[ax = b] \qquad (1.4)$$

$$a \equiv b \ (mód\ c) \Leftrightarrow (\exists x)[a = b + cx \ o \ a = b - cx] \qquad (1.5)$$

En esta última $A = 0 \ o \ B = 0 \ \Leftrightarrow A.B = 0, \qquad A = 0 \wedge B = 0 \leftrightarrow A^2 + B^2 = 0 \qquad (1.6)$

De (1.6) se sigue que las conjunciones y las disyunciones de relaciones diofánticas (pero no negaciones) son diofánticas. Procediendo de esta manera, podemos probar que muchas relaciones son diofánticas.

Una relación muy conocida es la de *coprimalidad*: a es coprimo con b sii $(a, b) = 1$. Esta relación puede ser considerada diofántica usando (1.5) de la siguiente manera:

$$a \perp b \iff (\exists x, y)[ax - by = 1 \; o \; ax - by = -1] \quad (1.7)$$

Otros ejemplos de funciones diofánticas son la *función resto* y la *función cociente*. Estas funciones se pueden considerar como diofánticas de la siguiente manera:

$$r = res(a, b) \iff r \equiv a \; (mód \; b) \quad y \quad r < b \quad (1.8)$$

$$q = coc(a, b) \iff 0 \leq a - qb < b. \quad (1.9)$$

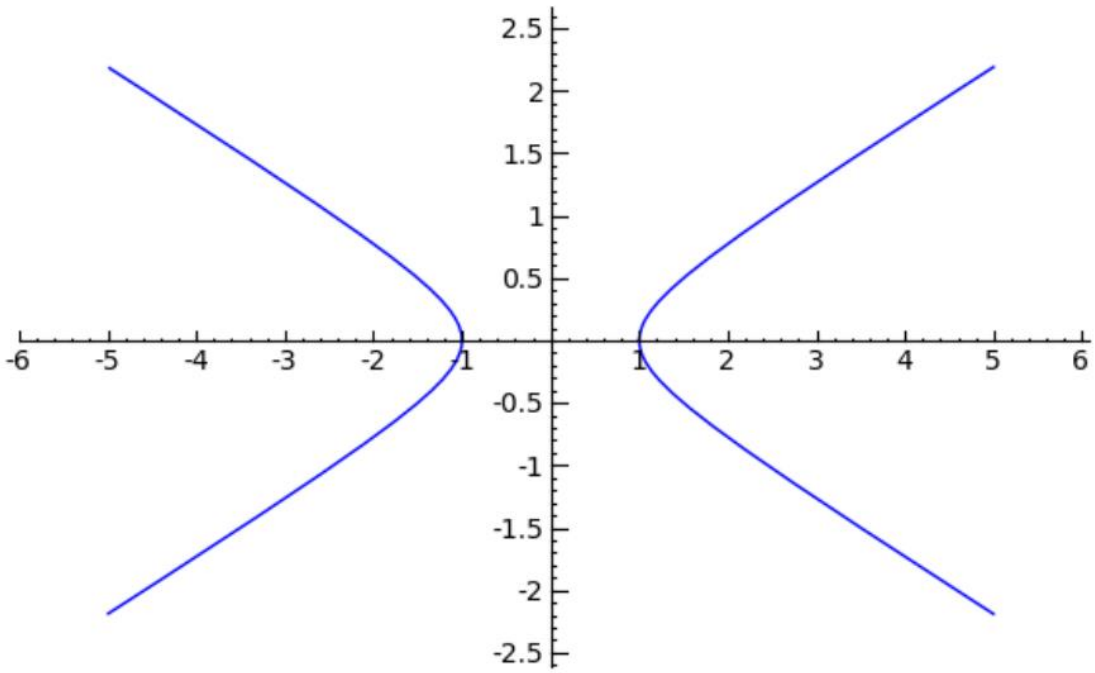
§2 La ecuación de Pell

A continuación desarrollaremos en profundidad un estudio de las soluciones de esta ecuación, las cuales serán centrales para la demostración del Teorema de Matijasevic, el cual nos permitirá resolver el décimo problema de Hilbert.

Definición 2.1: La ecuación general de Pell es una ecuación diofántica de la forma

$$x^2 - dy^2 = 1 \qquad (d \neq \blacksquare) \qquad (2.1)$$

donde d es una constante y x e y son incógnitas. (Una hipérbola en el plano (x, y).



Cuando $d = \blacksquare$ (d es un cuadrado), entonces la ecuación de Pell (2.1) tiene sólo la solución trivial $(1,0)$. Entonces siempre asumimos que $d \neq \blacksquare$ (d no es un cuadrado) así la ecuación tiene solución no trivial (distinta de $x = 1$ e $y = 0$).

Para realizar un estudio detallado de la ecuación de Pell primero necesitamos ver algunas definiciones básicas sobre su dominio de integración y sus componentes.

Dado que $x^2 - dy^2$ se puede descomponer en $x^2 - dy^2 = \left(x + \sqrt{d}y\right)\left(x - \sqrt{d}y\right)$, se puede trabajar en el dominio integral $Z\left[\sqrt{d}\right]$ de números reales de la forma $\alpha = x + y\sqrt{d}\ /\ \ x, y \in Z$, dado que $\sqrt{d}$ es irracional y los enteros x e y son únicos. Estos son las *componentes* de α.

Si $\alpha = x + y\sqrt{d}$ entonces su conjugado es $\bar{\alpha} = x - y\sqrt{d}$. Como sabemos de números complejos: $|Z|^2 = Z.\bar{Z}$. Entonces el número $N(\alpha) = \alpha\bar{\alpha} = x^2 - dy^2 = 1$ (por la ecuación de Pell) es la *norma* de α. Dado que $N(\alpha) = x^2 - dy^2 = 1$, las soluciones enteras a la ecuación de Pell son justamente las componentes enteras de x e y de reales α tal que $N(\alpha) = 1$. Esto último implica que $\alpha\bar{\alpha} = 1 \implies \alpha = \frac{1}{\bar{\alpha}}$.

Ahora sea $\alpha = x_1 + y_1\sqrt{d}$ y $\beta = x_2 + y_2\sqrt{d}$ dos soluciones de la ecuación de Pell, con x_1, y_1, x_2, y_2 enteros tales que $N(\alpha) = 1$ y $N(\beta) = 1$. Supóngase que $\alpha \geq 1$ y $\beta \geq 1$, entonces x_1, y_1, x_2, y_2 deben ser enteros no negativos. De las ecuaciones:

$$x_1^2 = dy_1^2 + 1 \qquad \text{y} \qquad x_2^2 = dy_2^2 + 1$$

se sigue que $$x_1 < x_2 \qquad \Leftrightarrow \qquad y_1 < y_2.$$

Entonces $1 \leq \alpha < \beta$ vale si y sólo si ambos $1 \leq x_1 < x_2$ y $0 \leq y_1 < y_2$ valen.

Entonces el conjunto de reales α para el cual $N(\alpha) = 1$ y $1 \leq \alpha$ se verifica, es un sistema bien ordenado. Si este conjunto es no vacío, es decir si existe una solución no trivial a la ecuación de Pell, entonces debe existir un mínimo real α tal que $1 \leq \alpha$ y $N(\alpha) = 1$. Este real α es llamado el *generador* y sus componentes son llamadas *solución fundamental*.

Las potencias del generador α generan todas las soluciones a (2.1). Para ver esto, primero observemos que $N(\alpha) = 1$ implica $N(\alpha^n) = N(\alpha)^{\,n} = 1$, entonces estas potencias de α representan soluciones. Para verificar que estas potencias de α dan todas las soluciones de (2.1), observemos que si $N(\beta) = 1$ y $1 \leq \beta$, entonces:

$\exists n \in N$ tal que $\alpha^n \leq \beta < \alpha^{n+1}$ (por las desigualdades nombradas más arriba).

Multiplicamos α^{-n} miembro a miembro obtenemos $1 \leq \beta.\alpha^{-n} < \alpha$.

Además, $N(\beta\alpha^{-n}) = N(\beta)N(\alpha^{-1})^n$ por propiedad de módulo

$N(\beta\alpha^{-n}) = N(\beta)N(\bar{\alpha})^n$ ya que $\alpha\bar{\alpha} = 1$

$N(\beta\alpha^{-n}) = N(\beta)N(\alpha)^n$ por ser $N(\alpha) = N(\bar{\alpha})$

$N(\beta\alpha^{-n}) = 1$ por $N(\alpha) = 1$ y $N(\beta) = 1$

Entonces se sigue que $\beta\alpha^{-n} = 1$ entonces $\beta = \alpha^n$. Por lo tanto β puede ser obtenido como una potencia de α.

No es enteramente trivial mostrar que para $d \neq \blacksquare$ arbitrario siempre existe una solución no trivial a la ecuación de Pell (2.1). Pero cuando d (no cuadrado) es de la forma especial $d = a^2 - 1$, entonces probaremos que existen infinitas soluciones. La ecuación de Pell (2.1) queda de la siguiente manera:

$$x^2 - (a^2 - 1)y^2 = 1 \qquad (2.2)$$

Esta tiene una solución fundamental en $(x, y) = (a, 1)$. Entonces el generador tal como lo habíamos definido $\alpha = x + y\sqrt{d}$ es $\alpha = a + \sqrt{a^2 - 1}$. Como expusimos más arriba las potencias del generador α generan todas las soluciones a (2.1), entonces:

$\beta = \alpha^n$ donde también es de la forma $\beta = x + y\sqrt{d}$

$$X_a(n) + Y_a(n).\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n \qquad (2.3)$$

$x = X_a(n)$ e $y = Y_a(n)$ denotan las secuencias de soluciones a (2.2), definidas por (2.3).

Ahora vamos a demostrar que las secuencias de soluciones $X_a(n)$ e $Y_a(n)$ son funciones estrictamente crecientes en n.

Como hemos definido más arriba $\bar{\alpha} = \alpha^{-1}$, el conjugado del generador es igual al inverso:

$$a - \sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^{-1} \qquad (2.4)$$

Entonces tomando los conjugados de ambos lados de (2.3) vemos que las secuencias $X_a(n)$ e $Y_a(n)$ son también definidas del conjugado del generador $a - \sqrt{a^2 - 1}$,

$$X_a(n) - Y_a(n).\sqrt{a^2 - 1} = (a - \sqrt{a^2 - 1})^n \qquad (2.5)$$

Esto implica que muchas de las identidades las cuales valen para las secuencias de soluciones de la ecuación de Pell también valen para valores negativos de parámetros. Además, de la aritmética sabemos que:

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

Por lo tanto, usando (2.3) obtenemos:

$X_a(n+m) + Y_a(n+m).\sqrt{a^2-1} = (a+\sqrt{a^2-1})^{n+m}$ y por la igualdad anterior:

$X_a(n+m) + Y_a(n+m).\sqrt{a^2-1} = (X_a(n) + Y_a(n).\sqrt{a^2-1}).(X_a(m) + Y_a(m).\sqrt{a^2-1})$

$X_a(n+m) + Y_a(n+m).\sqrt{d} = \left(X_a(n) + Y_a(n).\sqrt{d}\right).\left(X_a(m) + Y_a(m).\sqrt{d}\right)(\mathbf{1})$

En (2.5): $X_a(n-m) - Y_a(n-m).\sqrt{a^2-1} = (a-\sqrt{a^2-1})^{n-m}$

$X_a(n-m) - Y_a(n-m).\sqrt{a^2-1} = (X_a(n) - Y_a(n)\sqrt{a^2-1})(X_a(-m) - Y_a(-m)\sqrt{a^2-1})$

Pero por (2.4)

$a-\sqrt{a^2-1} = \left(a+\sqrt{a^2-1}\right)^{-1}$

$(a-\sqrt{a^2-1})^{m} = (a+\sqrt{a^2-1})^{-m}$

$(a-\sqrt{a^2-1})^{-m} = (a+\sqrt{a^2-1})^{m}$

La expresión anterior queda:

$X_a(n-m) - Y_a(n-m).\sqrt{a^2-1} = (X_a(n) - Y_a(n)\sqrt{a^2-1})(X_a(m) + Y_a(m)\sqrt{a^2-1})$

$X_a(n-m) - Y_a(n-m).\sqrt{d} = \left(X_a(n) - Y_a(n)\sqrt{d}\right)\left(X_a(m) + Y_a(m)\sqrt{d}\right) \quad (\mathbf{2})$

De (1) y (2):

$$X_a(n\pm m) \pm Y_a(n\pm m).\sqrt{d} = \left(X_a(n) \pm Y_a(n)\sqrt{d}\right)\left(X_a(m) + Y_a(m)\sqrt{d}\right)$$

Tomando las partes racionales e irracionales queda:

$$X_a(n\pm m) = X_a(n).X_a(m) \pm dY_a(n).Y_a(m) \qquad (2.6)$$

$$\pm Y_a(n\pm m) = X_a(n)Y_a(m) \pm Y_a(n)X_a(m)$$

$$Y_a(n\pm m) = Y_a(n)X_a(m) \pm X_a(n)Y_a(m) \qquad (2.7)$$

Haciendo $m = 1$, vemos también un caso especial:

$$X_a(n \pm 1) = X_a(n).X_a(1) \pm dY_a(n).Y_a(1)$$

$$X_a(n \pm 1) = X_a(n).a \pm dY_a(n) \quad (2.8)$$

$$Y_a(n \pm 1) = Y_a(n)X_a(1) \pm X_a(n)Y_a(1)$$

$$Y_a(n \pm 1) = Y_a(n)a \pm X_a(n) \quad (2.9)$$

Donde $X_a(1) = a$ y $Y_a(1) = 1$ y $X_a(0) = 1$ y $Y_a(0) = 0$

Por lo tanto: $X_a(n+1) = 2aX_a(n) - X_a(n-1)$ (2.8*)

$$Y_a(n+1) = 2aY_a(n) - Y_a(n-1) \quad (2.9^*)$$

Entonces $X_a(n)$ e $Y_a(n)$ son funciones estrictamente crecientes en n.

Generalmente estamos interesados en las secuencias X_a e Y_a solo para $a \geq 2$. Las ecuaciones (2.6) y (2.7) solo valen para $a \geq 2$ pero si definimos $X_1(n) = 1$ e $Y_1(n) = n$, entonces las expresiones anteriores valen para $a = 1$.

Ahora enunciaremos algunas propiedades y lemas que son necesarios para justificar el carácter diofántico de varias funciones que nos permitirá resolver el décimo problema de Hilbert.

- **Fórmulas del Ángulo Doble:**

De la ecuación (2.6) haciendo $m = n$ obtenemos:

$$X_a(n+n) = X_a(n).X_a(n) + dY_a(n).Y_a(n)$$

$$X_a(2n) = X_a(n)^2 + d\,Y_a(n)^2 \quad (2.10)$$

Por otro lado, como $X_a(n)$ e $Y_a(n)$ son soluciones de la Ecuación de Pell:

$$X_a(n)^2 - (a^2 - 1)Y_a(n)^2 = 1$$

$$X_a(n)^2 - dY_a(n)^2 = 1$$

$$dY_a(n)^2 = X_a(n)^2 - 1$$

Sustituyendo en (2.10)

$$\boxed{X_a(2n) = 2X_a(n)^2 - 1}$$

De forma similar en (2.7) con $m = n$

$$Y_a(n+n) = Y_a(n)X_a(n) + X_a(n)Y_a(n)$$

$$\boxed{Y_a(2n) = 2Y_a(n)X_a(n)}$$

- **Propiedad (2.11):** $\boldsymbol{n|m \leftrightarrow Y_a(n)|X_a(n)}$

De la ecuación (2.7) $Y_a(k \pm n) = Y_a(k)X_a(n) \pm X_a(k)Y_a(n)$

Obviando el subíndice a:

$$Y(k \pm n) - Y(k)X(n) = \pm X(k)Y(n)$$

Entonces:

$$Y(k \pm n) \equiv Y(k)X(n) \ (mód \ \ Y(n))$$

Pero $Y(n) \perp X(n)$ por (2.2): $x^2 - (a^2 - 1)y^2 = 1$

Entonces $Y(n)|Y(k \pm n) \Leftrightarrow Y(n).q = Y(k \pm n) \ /q \in Z$

Por (2.7) $Y(k \pm n) = Y(k)X(n) \pm X(k)Y(n)$

$$Y(n).q \mp X(k)Y(n) = Y(k)X(n)$$

$$Y(n).q' = Y(k)X(n)$$

Por lo tanto: $Y(n)|Y(k)X(n) \quad \Longrightarrow \quad Y(n)|Y(k).$

Ahora sea $m = ni + r \quad donde \quad 0 \leq r < n.$ entonces $0 \leq Y(r) < Y(n)$.

También $Y(n)|Y(m) \quad \Leftrightarrow \quad Y(n)|Y(ni + r) \quad \Leftrightarrow \quad Y(n)|Y(r)$ por lo anterior probado.

Por lo tanto $Y(n)|Y(m) \quad \Leftrightarrow \quad r = 0$ es decir $m = ni + 0$

Por lo tanto $Y(n)|Y(m) \quad \Leftrightarrow \quad n|m \ \therefore$

- **Primer paso Lema (2.12):** $\boldsymbol{Y_a^2(n)|Y_a(m) \quad \Leftrightarrow \quad n.Y_a(n)|m}$

Para la prueba de $\Longrightarrow$: suponemos que $Y_a^2(n)|Y_a(m)$

Por la propiedad (2.11) $m = nj$ para algún j.

Dado que $Y(n) \perp X(n)$ esto implica que

$$Y_a^2(n) | jY_a(n) \quad \rightarrow \quad Y_a(n) | j$$

Multiplicando a ambos lados por n tenemos

$$n.Y_a(n) | m \quad \therefore$$

Para la prueba de $\Longleftarrow$:

Usaremos dos veces la identidad (2.3):

$$X_a(n) + Y_a(n).\sqrt{a^2-1} = (a+\sqrt{a^2-1})^n \qquad \text{con} \qquad d = a^2 - 1$$

Para cualquier j

$$X_a(nj) + Y_a(nj).\sqrt{d} = (a+\sqrt{d})^{nj}$$

Pero $\quad (a+\sqrt{d})^{nj} = \left((a+\sqrt{d})^n\right)^j = (X_a(n) + Y_a(n).\sqrt{d})^j$

Entonces: $\quad X_a(nj) + Y_a(nj).\sqrt{d} = (X_a(n) + Y_a(n).\sqrt{d})^j \qquad (2.13)$

Luego desarrollamos con el Binomio de Newton el lado derecho de (2.13) y tomamos la parte irracional, nos queda:

$$Y_a(nj) = \sum_{i\ impar}^{j} \binom{j}{i} X_a(n)^{j-i} Y_a(n)^i (\sqrt{d})^{i-1}$$

Si $i = 1$

$$Y_a(nj) = \sum_{1}^{j} \binom{j}{1} X_a(n)^{j-1} Y_a(n)^1 (\sqrt{d})^{1-1}$$

Desarrollando:

$$Y_a(nj) = jX_a(n)^{j-1}Y_a(n) + \binom{j}{3} X_a(n)^{j-3} Y_a(n)^3 (\sqrt{d})^{3-1} + \cdots + \binom{j}{i} X_a(n)^{j-i} Y_a(n)^i (\sqrt{d})^{i-1}$$

$$Y_a(nj) - jX_a(n)^{j-1}Y_a(n) = Y_a(n)^3 q + \cdots + Y_a(n)^i q^{i'} \ \ / \ q \in Z$$

$$Y_a(nj) - jX_a(n)^{j-1}Y_a(n) = Y_a(n)^3 (q + \cdots + Y_a(n)^{i-3} q^{i'})$$

$$Y_a(nj) \equiv jX_a(n)^{j-1}Y_a(n) \ (mód \ \ Y_a(n)^3) \quad (2.14)$$

Ahora suponemos según nuestra hipótesis que

$$n.Y_a(n)|m$$

Sea $j = Y(n)$. Este j es el de (2.14) sustituyendo en la misma:

$$Y_a(n.Y(n)) \equiv Y(n)X_a(n)^{Y(n)-1}Y_a(n)\ (mód\ \ Y_a(n)^3)$$

Entonces

$$Y_a(n.Y(n)) \equiv Y(n)^2X_a(n)^{Y(n)-1}\ (mód\ \ Y_a(n)^3)$$

$$Y_a\big(n.Y(n)\big) = Y(n)^2X_a(n)^{Y(n)-1} + Y_a(n)^3.q\ \ /q \in Z$$

$$Y_a\big(n.Y(n)\big) = Y(n)^2\big(X_a(n)^{Y(n)-1} + Y(n).q\big)$$

Por lo tanto $\quad Y(n)^2|Y_a\big(n.Y(n)\big)\ \therefore$

- **Segundo Paso Lema (2.15):** $\boldsymbol{Y_a(k) \equiv \pm Y_a(m)\ \big(mód\ X_a(n)\big) \Leftrightarrow k \equiv \pm m\ (mód\ 2n)}$

Asumiremos que $a \geq 2,\ n \geq 1$.

Para la prueba de $\Longleftarrow$:

Suponemos que $k = 2nj \pm m$ ya que por hipótesis $k \equiv \pm m\ (mód\ 2n)$

$$Y(k) = Y(2nj \pm m) = Y(2nj)X(m) \pm X(2nj)Y(m)$$

Utilizando las Fórmulas del Angulo Doble:

$$Y(k) = Y(2nj \pm m) = 2X(nj)Y(nj)X(m) \pm (2X(nj)^2 - 1)Y(m)$$

$$Y(k) = Y(2nj \pm m) = 2X(nj)Y(nj)X(m) \pm 2X(nj)^2Y(m) \mp Y(m)$$

$$Y(k) = Y(2nj \pm m) = \mp Y(m) + X(nj)[2Y(nj)X(m) \pm X(nj)Y(m)]$$

$$Y(k) \equiv \mp Y(m)(mód\ X(n))$$

Cuando $j = 2i$, tenemos:

$$Y(k) = Y(4ni \pm m) \equiv Y(m)\big(mód\ \ X(n)\big).$$

En este caso $j = 2i + 1$, tenemos:

$$Y(k) = Y(4ni + 2n \pm m) \equiv Y(m)\big(mód\ \ X(n)\big).$$

Entonces: $Y_a(k) \equiv \pm Y_a(m) \ \left(mód\ X_a(n)\right) \therefore$

Para la prueba de $\Longrightarrow$:

Asumimos por hipótesis que $Y_a(k) \equiv \pm Y_a(m) \ \left(mód\ X_a(n)\right)$

Eligiendo un k' tal que $0 \leq k' \leq n$ y $k \equiv \pm k'\ (mód\ 2n)$

También eligiendo un m' tal que $0 \leq m' \leq n$ y $m \equiv \pm m'(mód\ 2n)$

Por hipótesis tenemos que:

$$Y_a(k') \equiv \pm Y_a(m') \ \left(mód\ X_a(n)\right)$$

$$Y_a(k') = \pm Y_a(m') + X_a(n).q \quad /q \in Z$$

$$Y_a(k') \pm Y_a(m') = X_a(n).q$$

$$X_a(n) | Y_a(k') \pm Y_a(m')$$

Vamos a demostrar que $k' = m'$ por el absurdo:

Suponemos que $k' \neq m'$ entonces deberíamos tener:

$$0 < |Y_a(k') \pm Y_a(m')| \leq |Y_a(k') + Y_a(m')| \leq Y_a(n-1) + Y_a(n) \quad (1)$$

Ya que $k' \leq n-1$ y $m' \leq n$ según nuestra hipótesis

Por otro lado, utilizando (2.9) sustituyendo n por $n-1$, tenemos:

$$Y(n) = a.Y(n-1) + X(n-1)$$

Como sabemos $2 \leq a$, entonces:

$$2.Y(n-1) \leq a.Y(n-1) < a.Y(n-1) + X(n-1) = Y(n)$$

$$2.Y(n-1) < Y(n)$$

$$Y(n-1) < Y(n) - Y(n-1)$$

Entonces sumando a ambos lados $Y(n)$, tenemos:

$Y(n-1) + Y(n) < 2.Y(n) - Y(n-1) \leq a.Y(n) - Y(n-1) = a.Y(n) - a.Y(n) + X(n) = X(n)$ En el último paso utilizamos (2.9) nuevamente.

Por lo tanto, $Y(n-1) + Y(n) < X(n)$ (2)

De (1) y (2): $|Y_a(k') \pm Y_a(m')| < X(n)$. Absurdo ya que según nuestra hipótesis:

$$X_a(n)|Y_a(k') \pm Y_a(m')$$

Por lo tanto, $k' = m'$ por lo que deducimos que $k \equiv \pm m \ (mód\ 2n)$ ∴

El siguiente lema es esencial para justificar el carácter diofántico de varias funciones el cual nos llevará a resolver el décimo problema de Hilbert.

- **Lema (2.16):**

$\boldsymbol{Para\ A} > 1. En\ orden\ C = \boldsymbol{Y_A(B)}$,

$\boldsymbol{es\ necesario\ y\ suficiente\ que\ existan\ n}$$\boldsymbol{úmeros\ naturales\ D, E, F, G, H, I\ e\ i\ tal\ que}$

$(\mathbf{1})\ \boldsymbol{D^2 - (A^2 - 1)C^2 = 1}$,

$(\mathbf{2})\ \boldsymbol{F^2 - (A^2 - 1)E^2 = 1}$,

$(\mathbf{3})\ \boldsymbol{I^2 - (G^2 - 1)H^2 = 1}$,

$(\mathbf{4})\ \boldsymbol{E = (i + 1)2C^2}$,

$(\mathbf{5})\ \boldsymbol{G \equiv A\ (mód\ F)}$,

$(\mathbf{6})\ \boldsymbol{G \equiv 1\ (mód\ 2C)}$,

$(\mathbf{7})\ \boldsymbol{H \equiv C\ (mód\ F)}$,

$(\mathbf{8})\ \boldsymbol{H \equiv B\ (mód\ 2C)}$,

$(\mathbf{9})\ \boldsymbol{B \leq C}$.

Prueba de suficiencia: Supóngase que existen *D, E, F, G, H, I, i* que satisfacen (1)-(9).

Entonces las ecuaciones (1)-(3), ecuaciones de Pell, implican la existencia de números $p, q\ r$ tal que:

$$D = X_A(p), \qquad C = Y_A(p), \qquad F = X_A(q),$$

$$E = Y_A(q), \qquad I = X_G(r), \qquad H = Y_G(r).$$

También tenemos $0 \leq p \leq C$ y $0 \leq B \leq C$.

Por lo tanto la idea es mostrar que $B = p$, probando que $B \equiv r \equiv \pm p\ (mód\ 2C)$.

Podemos suponer que $0 < C$. Usando el Primer Paso Lema (2.12), junto con (4), tenemos:

$$C^2 \big| E \ \rightarrow\ Y_A^2(p) \big| Y_A(q) \Longrightarrow\ Y_A(p)|q\ \Longrightarrow C|q.$$

Para mostrar que $B \equiv r\ (mód\ 2C)$, usaremos (6) y (8):

$$B \equiv H = Y_G(r)$$

$Y_G(r)$ es un polinomio en G por lo tanto: $Y_G(r) \equiv Y_1(r)\ (mód\ G-1)$

Por (6): $G-1=2C \quad \rightarrow\ Y_G(r) \equiv Y_1(r)\ (mód\ 2C) = r\ (mód\ 2C)$ usando $Y_1(r) = r$

Entonces $B \equiv r\ (mód\ 2C)$ **(*1)**

Por el Segundo Paso Lema (2.15), (5) y (7), y lo antes mencionado:

$$Y_A(r) \equiv Y_G(r) = H \equiv C = Y_A(p)\ \big(mód\ \ F = X_A(q)\big) \Longrightarrow r \equiv \pm p\ \ (mód\ 2q).$$

En la última implicación aplicamos el Segundo Paso.

Pero $C|q$. De ahí $r \equiv \pm p\ \ (mód\ 2C)$. Esto último y por **(*1)** implica:

$$B \equiv \pm p\ (mód\ 2C)$$

Prueba de Necesidad:

Suponga que $C = Y_A(B)$. Sea $D = X_A(B)$. Entonces (1) y (9) valen.

Puesto que $q = B.Y_A(B), F = X_A(2q)\ \ e\ \ E = Y_A(2q)$.

Sustituyendo en (2): $\quad X_A(2q)^2 - (A^2-1)Y_A(2q)^2 = 1$

Entonces (2) vale.

Sea $m = B.Y_A(B)$ en el Primer Paso Lema (2.12) entonces implica que:

$$Y_A(B)^2 | Y_A\big(B.Y_A(B)\big)$$

Y en concordancia con lo que dijimos más arriba $C^2|E \ \ \Longrightarrow C^2|Y_A(q)$. Por las fórmulas del Angulo Doble:

$$2Y_A(q)X_A(q) = Y_A(2q).$$

De ahí que $\quad C^2.z = Y_A(q)/z \in Z\ \rightarrow\ C^2.z.2X_A(q) = Y_A(q)\ \ 2X_A(q)$ multiplicando $2X_A(q)$ miembro a miembro y sustituyendo por la igualdad anterior:

$$C^2.z.2X_A(q) = Y_A(2q)$$

$2C^2|Y_A(q)\ \Longrightarrow\ 2C^2|E$. Por lo tanto (4) puede ser satisfecho.

Haciendo $G = A + F^2(F^2 - A)$. Entonces (5) vale.

Sustituyendo (4) en (2):

$$F^2 - (A^2 - 1)(i + 1)^2 4C^2 = 1$$

Lo que implica que: $F^2 \equiv 1 \ (mód\ 2C)$.

Entonces $G = A + F^2(F^2 - A)$ implica (6).

Haciendo $I = X_G(B)$ y $H = Y_G(B)$. Entonces, de forma similar como demostramos (2), (3) vale.

Como dijimos más arriba, $Y_G(B)$ es un polinomio en G por lo tanto:

$$Y_G(B) \equiv Y_1(B) \equiv B \ (mód\ G - 1)$$

Entonces por (6) $H \equiv B \ (mod\ 2C)$ por lo tanto (8) vale.

Puesto que $Y_G(B)$ es un polinomio en G y $Y_A(B)$ es un polinomio en A entonces:

$$Y_G(B) \equiv Y_A(B) \ (mód\ G - A)$$

Y por (5): $G \equiv A \ (mód\ F) \Longrightarrow G - A = F$

Entonces como $B \equiv r \equiv \pm p \ \ (mód\ 2C)$:

$$H = Y_G(B) \equiv Y_A(B) = C \ (mód\ G - A)$$

$$H \equiv C \ \ (mód\ F).$$

Por lo tanto (7) vale.∴

§3 Funciones diofánticas.

Para probar el Teorema de Matijasevic, el cual es central para resolver el Décimo Problema de Hilbert, necesitamos justificar el carácter diofántico de varias funciones. La más importante de ellas es la función exponencial que fue demostrada por Matijasevic en 1970.

- *La función exponencial*

Del Lema (2.16) demostrado en el apartado anterior y de la ecuación de Pell (2.2) sabemos que $x = X_a(n)$ e $y = Y_a(n)$ son relaciones diofánticas y estas están implicadas en las ecuaciones

de congruencia enunciadas en el Lema (2.16). Esto lo utilizaremos para demostrar que la función exponencial es diofántica.

Lema 3.1: $\boldsymbol{Suponga\ que\ n \geq 1, k \geq 2}$.

$\boldsymbol{Para\ a\ suficientemente\ grande\ tal\ que\ a \geq Y_k(n+1)}$:

$$\boxed{\boldsymbol{k^n = res\big(X_a(n) - (a-k)Y_a(n), 2ak - k^2 - 1\big)}}$$

Demostración:

Sabemos que si $Y_a(n)$ es un polinomio en a de grado $n-1$, entonces $Y_a(n+1)$ es un polinomio en a de grado n.

Para demostrar este lema primero demostraremos la siguiente desigualdad por inducción sobre n:

$$(2a-1)^n \leq Y_a(n+1) \leq (2a)^n$$

Para $n = 1$. $(2a-1) \leq Y_a(2) \leq (2a)$

Por las fórmulas del ángulo doble $Y_a(2) = 2.Y_a(1).X_a(1) = 2.1.a = 2a$

Se verifica para $n = 1$.

Para $n = k$ hipótesis inductiva:

$$(2a-1)^k \leq Y_a(k+1) \leq (2a)^k$$

Veamos que la desigualdad es válida para $n = k+1$

Usando que $Y_a(n)$ es una sucesión estrictamente creciente y la hipótesis de inducción, tenemos que:

$$\begin{aligned}(2a-1)^{k+1} &= (2a-1)(2a-1)^k < (2a-1)Y_a(k+1) = 2aY_a(k+1) - Y_a(k+1) \\ &< 2aY_a(k+1) - Y_a(k) < 2a(2a)^k - Y_a(k) = (2a)^{k+1} - Y_a(k) < (2a)^{k+1}\end{aligned}$$

Luego $(2a-1)^{k+1} < 2aY_a(k+1) - Y_a(k) < (2a)^{k+1}$

Pero por la ecuación (2.7) y las fórmulas del ángulo doble:

$$\begin{aligned}Y_a(k+2) &= Y_a(k).X_a(2) + X_a(k).Y_a(2) \\ &= Y_a(k)(2a^2-1) + X_a(k).2a = 2a\big(aY_a(k) + X_a(k)\big) - Y_a(k)\end{aligned}$$

Por la ecuación (2.9): $aY_a(k) + X_a(k) = Y_a(k+1)$

Entonces: $Y_a(k+2) = 2aY_a(k+1) - Y_a(k)$ con lo que la desigualdad queda probada.

Volviendo al lema (3.1) para nuestro caso:

$k \leq k^n < (2k-1)^n \leq Y_k(n+1) \leq a$. Por hipótesis

Se sigue que $k + 1 \leq a,$ (*)

y también

$$1 < k$$

$$a + 1 < k.(a+1)$$

$$a < k.(a+1) - 1$$

$$a < ak + k - 1$$

De ahí:

$a.k + k - 1 = ak + (k+1)k - k^2 - 1 \leq ak + ak - k^2 - 1 = 2ak - k^2 - 1$. Por (*)

Por lo tanto: $k^n < a < 2ak - k^2 - 1$. Entonces k^n es más pequeño que el módulo.

Ahora tenemos que demostrar una congruencia obtenida por Julia Robinson en 1952.

$$k^n \equiv X_a(n) - (a-k)Y_a(n) \ (mód\ 2ak - k^2 - 1) \quad (3.2)$$

Usaremos las ecuaciones (2.8*) y (2.9*) e inducción sobre n, es decir que la ecuación (3.2) es nuestra hipótesis inductiva.

$$\begin{aligned} X_a(n+1) - (a-k)Y_a(n+1) = \ & 2aX_a(n) - X_a(n-1) - (a-k)[2aY_a(n) - Y_a(n-1)] \\ &= 2a[X_a(n) - X_a(n-1)] - [X_a(n-1) - (a-k)Y_a(n-1)] \\ &\equiv 2ak^n - k^{n-1} = k^{n-1}(2ak-1) = k^{n-1}(2ak - k^2 - 1 + k^2) \\ &\equiv k^{n-1}(0 + k^2) = k^{n-1}k^2 = k^{n+1} \ (mód\ 2ak - k^2 - 1) \ \therefore \end{aligned}$$

Entonces por (3.2) y dado que k^n es más pequeño que el módulo, por lo tanto k^n es el resto, lo cual queríamos demostrar.

En la sección 1 vimos que la función resto tiene el carácter de función diofántica y ya que la función exponencial la expresamos como tal, entonces el Lema (3.1) y junto con lo expuesto sobre el Lema (2.16) implican que $m = k^n$ es diofántica.

- *El coeficiente binomial*

Julia Robinson definió las funciones exponencial-diofánticas como las definibles en términos de ecuaciones diofánticas y de la función exponencial y probó que las funciones que vamos a estudiar ahora eran exponencial-diofánticas. Ahora demostramos que los números combinatorios son diofánticos.

Lema 3.3. $\boldsymbol{Para\ k \geq 0, n\ \ y\ \ u > 2^n}$,

$$\boldsymbol{\binom{n}{k} = res\left(\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor, u\right)}$$

Demostración:

Desarrollamos $(u+1)^n$ por el Binomio de Newton

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

y dividimos a todo por u^k,

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

Por otro lado sabemos que $u^{i-k} \leq \frac{1}{u}$, la cual vale para $i \leq k-1$, junto con (3.3) tenemos

$$\sum_{i=0}^{k-1} \binom{n}{i} u^{i-k} \leq \sum_{i=0}^{k-1} \binom{n}{i} \frac{1}{u} \leq \frac{1}{u} \sum_{i=0}^{n} \binom{n}{i} = \frac{2^n}{u} < 1$$

Por lo tanto la parte entera es

$$\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor = \binom{n}{k} + \sum_{i=k+1}^{n} \binom{n}{i} u^{i-k} = \binom{n}{k} + u \sum_{i=k+1}^{n} \binom{n}{i} u^{i-k-1} \equiv \binom{n}{k}\ (mód\ u) \therefore$$

Además, del Lema (3.3) se sigue que $\binom{n}{k} \leq 2^n < u$

Del Lema (3.1) sabemos que la función exponencial es diofántica, por lo tanto $(u+1)^n$ y u^k son diofánticas. Además, de la sección 1 sabemos que la función cociente también es diofántica así que $\frac{(u+1)^n}{u^k}$ es diofántica. Por último, como la función resto es diofántica entonces el coeficiente binomial es diofántico.

§4 Conjuntos y funciones recursivas

Ahora tenemos bastantes funciones y relaciones diofánticas para poder demostrar el Teorema de Matijasevic que nos permitirá resolver el Décimo problema de Hilbert. Antes de desarrollar el mencionado teorema debemos incluir algunas definiciones sobre funciones y conjuntos que serán de gran utilidad para nuestro propósito.

- *Funciones recursivas*

Las funciones recursivas resultan ser exactamente las funciones calculables mediante un algoritmo. Por "un algoritmo" entendemos cualquier secuencia finita de instrucciones que nos permita obtener tras un número finito de cálculos mecánicos el valor que toma la función sobre unos argumentos dados (el número de pasos necesarios puede depender de la magnitud de los argumentos). Veamos primero algunas definiciones auxiliares para luego ver la definición formal.

Funciones recursivas elementales: Llamaremos funciones recursivas elementales a las siguientes funciones:

* La función monádica c, dada por $c(n) = 0$ para todo n.

* La función monádica s, dada por $s(n) = n + 1$ para todo n.

* Las funciones k-ádicas p^k para $1 \leq i \leq k$ dadas por $p_i^k(n_1, \dots, n_k) = n_i$

Observar que todas las funciones recursivas elementales se pueden calcular explícitamente en cada caso concreto. Las funciones recursivas son las que pueden obtenerse a partir de estas mediante la aplicación de un número finito de los procesos de definición los cuáles son los siguientes:

a) Una función k-ádica f está definida por **composición** a partir de la función r-ádica g y de las funciones k-ádicas $h_1, \dots, h_r$ si y sólo si para todos los naturales $a_1, \dots, a_k$ se cumple que

$$f(a_1, \dots, a_k) = g(h_1(a_1, \dots, a_k), \dots, h_r(a_1, \dots, a_k))$$

Si tenemos funciones g y $h_1, \dots, h_r$, la ecuación anterior determina una función f sin ambigüedad alguna.

b) Una función $k+1$-ádica f está definida por **recursión** a partir de la función k-ádica g (o del natural a si $k = 0$) y de la función $k+2$-ádica h si y sólo si para todos los naturales $a_1, \dots, a_k, n$ se cumple que

$$f(0, a_1, \dots, a_k) = g(a_1, \dots, a_k) \ \ [f(0) = a, si\ k = 0]$$

$$f(n+1, a_1, \dots, a_k) = h(n, f(n, a_1, \dots, a_k), a_1, \dots, a_k).$$

Si tenemos funciones g, h (o un número a y una función h), las ecuaciones anteriores determinan unívocamente una función f. Si disponemos de algoritmos para calcular g y h también tenemos otro para calcular f.

c) Una función k-ádica f está definida por **minimización** a partir de una función $k + 1$-ádica g si para todos los naturales $a_1, \dots, a_k$ se cumple

1. $\forall n\ g(a_1, \dots, a_k, n) = 0$

2. $f(a_1, \dots, a_k) = \mu n\ g(a_1, \dots, a_k, n) = 0$ $\qquad$ μn significa "el mínimo natural n"

Dada una función g que cumpla 1), la ecuación 2) determina unívocamente una función f que será calculable mediante un algoritmo si lo es g.

Ahora si daremos la definición formal de función recursiva.

Definición 4.1: Una función f es **recursiva primitiva (recursiva)** si existe una sucesión de funciones $f_1, \dots, f_n$ tales que f_n es f y para todo natural i entre 1 y n, la función f_i está definida por composición, recursión o minimización a partir de funciones anteriores de la sucesión.

Es claro que toda función recursiva primitiva es recursiva y la única diferencia entre las funciones recursivas y las recursivas primitivas consiste en que en las primeras se admite la minimización como técnica de definición y en las segundas no.

Además toda función recursiva es calculable mediante un algoritmo. Más concretamente, si f es una función recursiva, una sucesión de funciones $f_1, \dots, f_n$ según la definición determina un algoritmo para calcular f (en el sentido de que conociendo la sucesión es fácil diseñar el algoritmo correspondiente). Más aún, Turing demostró que las funciones recursivas son exactamente las calculables mediante un algoritmo. Esta afirmación se conoce como Tesis de Church-Turing y la probaremos en la sección siguiente.

Veamos un ejemplo donde apliquemos las diferentes funciones recursivas elementales y los procesos de definición de recursión y composición.

Ejemplo 4.2: *La suma de números naturales es una función diádica recursiva primitiva*.

Demostración:

$h_1(m) = m$ Función 1-ádica p_1^1

$h_2(m,n,p) = p$ Función 3-ádica p_3^3

$h_3(m) = m + 1$ Función monádica s

$h_4(m,n,p) = h_3\big(h_2(m,n,p)\big) = p + 1$ Por composición

$h_5(m,0) = h_1(m) = m$ Por recursión

$h_5(m,n+1) = h_4\big(m,n,h_5(m,n)\big) = h_5(m,n) + 1$

Claramente $h_5(m,n) \ = \ m + \ n$.

Otros ejemplos de funciones recursivas: Todas estas son funciones recursivas porque están definidas por composición, recursión o minimización de funciones anteriores en la sucesión.

1) $m.n$ $\quad m.0 = 0 \quad m.(n+1) = m.n + m$

2) $C_a(n) = a$ $\quad C_a(0) = a \quad C_a(n+1) = C_a(n)$

3) m^n $\quad m^0 = 1 \quad m^{n+1} = m^n.m$

4) $n!$ $\quad 0! = 1 \quad (n+1)! = n!.(n+1)$

5) $pre(n)$ $\quad pre(0) = 0 \quad pre(n+1) = n$

Definición 4.3: Una función recursiva primitiva (recursiva) es de **rango** n si puede definirse en n pasos sin usar proyecciones p_i^k con $k > n$. Es claro que sólo hay un número finito de tales funciones, pues sólo hay una cantidad finita de funciones elementales de las que podamos partir y sólo hay un número finito de posibilidades de combinar los dos métodos de construcción de funciones en n pasos.

Ejemplo: Como vimos más arriba la función factorial es recursiva. El rango de $n!$ es n, ya que esta se define en n pasos por composición de la función multiplicación:

$$n! = n.(n-1)! = n.(n-1).(n-2)! = \cdots = n.(n-1).(n-2) \ldots 3.2.1$$

- *Conjuntos recursivos*

Definimos ahora los conjuntos recursivos. Intuitivamente sabemos que los conjuntos recursivos son los listables. Cuando hayamos probado la tesis de Church-Turing veremos que un conjunto es recursivo si existe un algoritmo que determina si un número natural dado pertenece o no al conjunto.

Definición 4.4: Sea A un conjunto de números naturales. Llamaremos *función característica* de A a la función monádica dada por

$$X_A(n) = \begin{cases} 1 & \text{si } n \text{ está en } A \\ 0 & \text{si } n \text{ no está en } A \end{cases}$$

Diremos que el conjunto A es **recursivo** (primitivo) si la función X_A es recursiva (primitiva).

Es decir que un conjunto es recursivo si tenemos un medio para determinar si un elemento pertenece o no a dicho conjunto.

Teorema 4.5: *Todo conjunto finito es recursivo primitivo*.

Demostración:

Veamos primero que si k es un número natural, el conjunto $\{k\}$ es recursivo primitivo. Ello se debe a que la función dada por $f(x) = x$ si y sólo si $x = k$ es recursiva primitiva ya que $x = k$ puede escribirse como la función k-ádica $p_1^1(x) = x$ y claramente $X_{\{k\}}(x) = p_1^1(x)$

Para un conjunto $A = \{k_1, \ldots, k_n\}$ tenemos que $X_A = X_{\{k_1\}}, \ldots, X_{\{k_n\}}$. A es recursivo.

Ejemplo: El conjunto de las potencias de 2 es un conjunto recursivo.

Dada la función $f(n) = 2^n \ /n \in N$. Esta función es recursiva ya que está definida por composición de funciones primitivas: es el doble del anterior en la sucesión.

$$f_1(n_1) = 2^{n_1}$$

$$f_2(n_2) = 2.f_1(n_1) = 2.2^{n_1}$$

f puede escribirse como la función k-ádica $p_1^1(n) = 2^n$.

Si llamamos A al conjunto $A = \{2^1, 2^2, 2^3 \ldots, 2^n\}$, entonces $X_A(n) = p_1^1(n) = 2^n$. Por lo tanto A es recursivo.

Definición 4.6: Un conjunto de números naturales A es **recursivamente numerable (r.e.)** si es la imagen de una función monádica recursiva o si A coincide con el rango exacto de una función recursiva.

Ejemplo: El conjunto anterior definido $A = \{2^1, 2^2, 2^3 \dots, 2^n\}$ es recursivamente enumerable.

Como dijimos en el ejemplo anterior $f(n) = 2^n \ /n \in N$ es recursiva. El rango de f es n ya que para obtener el número 2^n en la sucesión la función f debe componerse n veces como lo detallamos en el ejemplo anterior.

Entonces, $A = rang(f) = \{f(1), f(2), f(3), \dots, f(n)\}$. Por lo tanto A es r.e.

Teorema 4.7: Todo conjunto recursivo es recursivamente enumerable.

Demostración: Por definición A es recursivo $\rightarrow$ X_A es monádica recursiva. Esta función lista todos los elementos de A. Entonces A es la imagen de una función monádica recursiva. Por lo tanto A es recursivamente enumerable.

Sin embargo, existen conjuntos recursivamente enumerables los cuales no son recursivos.

A fin de dar un ejemplo para mostrar que no siempre vale la doble implicación del teorema 4.7 ahondaremos aún más en la teoría de la recursión. Para el sólo hecho de demostrar la existencia de algún ejemplo daremos algunas definiciones básicas.

Sea $A \subset X$. Diremos que A es *productivo* si existe una función recursiva f tal que

$$\forall x(W_x \subset A \Longrightarrow f(x) \in A - W_x)$$

La función f se llama función productiva de A.

Entonces: A es productivo $\Longrightarrow A$ no es r.e. Si $W_x \subset A$ entonces $W_x \cup \{f(x)\}$ es un conjunto r.e.

Por otro lado, A es *creativo* si es r.e. y $\bar{A}$ es productivo

Un conjunto productivo es un conjunto para el que la prueba de ser no r.e. se realiza recursivamente. Un conjunto creativo es un conjunto r.e. para el que la prueba de ser no recursivo se realiza recursivamente por medio de una función productiva de su complementario.

Entonces, A es creativo $\Longrightarrow A$ es r.e. pero no recursivo.

Con estas definiciones estamos en condiciones de dar un ejemplo concreto:

$K = \{x: x \in W_x\}$ no es productivo, ya que como dijimos previamente es r.e.

$\overline{K} = \{x: x \notin W_x\}$ es productivo por definición ya que $\overline{K}$ no es r.e.

K es creativo pues es r.e. y su complemento es productivo. Entonces, K es r.e. pero no recursivo.

Teorema 4.8: Un conjunto A es recursivo si y solo si A y su complemento $\bar{A}$ son ambos conjuntos recursivamente enumerables.

Demostración:

$\Longrightarrow$:

A es recursivo $\Longrightarrow$ A es r.e. (Por el teorema 4.7)

A es recursivo, por lo tanto por definición de conjunto recursivo:

$$X_A(n) = \begin{cases} 1 & si\ n \in A \\ 0 & si\ n \notin A \end{cases}$$

Negando miembro a miembro

$$X_{\bar{A}}(n) = \begin{cases} 0 & si\ n \notin A \\ 1 & si\ n \in A \end{cases}$$

Por lo tanto, por definición, $\bar{A}$ es recursivo $\Longrightarrow$ $\bar{A}$ es r.e. (Por el teorema 4.7).

$\Longleftarrow$:

A es r.e. $\Longrightarrow$ $\exists f(n)$ recursiva que tiene como imagen al conjunto A.

$\bar{A}$ es r.e. $\Longrightarrow$ $\exists g(n)$ recursiva que tiene como imagen al conjunto $\bar{A}$.

Armo una función característica:

$$X_A(n) = \begin{cases} 1 & \text{si } n \text{ pertenece a la imagen de } f \\ 0 & \text{si } n \text{ pertenece a la imagen de } g \end{cases}$$

Considerando las funciones f y g definidas:

$$X_A(n) = \begin{cases} 1 & si\ n \in A \\ 0 & si\ n \notin A \end{cases}$$

Por definición, A es recursivo.

- *Funciones parciales*

Para luego demostrar la tesis de Church-Turing necesitamos introducir una clase más general de funciones: las funciones parciales. Estas son necesarias para comprobar si una función es recursiva o no.

Veamos primero un ejemplo donde disponemos de un algoritmo para calcular $f_m(n)$ para cualquier par de números m y n. Recordando la definición de rango de una función recursiva, sólo tenemos que enumerar todas las funciones de rango 1 y contar todas las que sean monádicas, luego todas las de rango 2, etc. hasta que la suma total de funciones monádicas iguale o exceda a m. Entonces, si esto ha sucedido al considerar las funciones de rango k, las ordenamos según el criterio explícito prefijado para las definiciones y nos quedamos con la definición de la función monádica que hace el número de orden m. Esta es f_m y, como tenemos su definición, a partir de ella podemos calcular $f_m(n)$. De este modo, tenemos definida una función diádica $f(m,n) = f_m(n)$ que sabemos calcular mediante un algoritmo. De hecho, es posible precisar todos los cálculos que hemos descrito para calcular f explícitamente y comprobar que satisface la definición de función recursiva.

Sin embargo, no disponemos de ningún algoritmo para enumerar explícitamente las sucesiones que definen funciones recursivas y el problema está en las definiciones por minimización, ya que no sabemos si cumple o no la condición requerida en este proceso de definición. Aunque podamos enumerar todas las "posibles" definiciones de funciones recursivas de rango k, como hicimos en el ejemplo, no está claro que sepamos distinguir cuáles de ellas son válidas.

El hecho de no saber si una definición es correcta o no, es un inconveniente técnico que necesitamos resolver, para lo cual introducimos las funciones parciales.

Una *función parcial* n-ádica f es un criterio bien definido que a ciertos grupos de n naturales $a_1, \dots, a_n$ repetidos o no y en un cierto orden les asigna otro número natural que representaremos por $f(a_1, \dots, a_n)$. Diremos en este caso que f está definida para $a_1, \dots, a_n$ o que $f(a_1, \dots, a_n)$ está definido.

Así como las funciones recursivas son las que pueden obtenerse a partir de las elementales mediante la aplicación de un número finito de los procesos de definición, los mismos son los que se utilizan para las funciones parciales y son los siguientes:

a) Una función parcial k-ádica está definida por **composición parcial** a partir de las funciones parciales g (r-ádica) y $h_1, \dots, h_r$ (k-ádicas) si f está definida exactamente para aquellos naturales $a_1, \dots, a_k$ tales que están definidas

$h_i(a_1, \dots, a_k)(i = 1, \dots, r)$ y $g(h_1(a_1, \dots, a_k), \dots, h_r(a_1, \dots, a_k))$ y se cumple

$$f(a_1, \dots, a_k) = g(h_1(a_1, \dots, a_k), \dots, h_r(a_1, \dots, a_k))$$

b) Una función parcial $k + 1$-ádica está definida por **recursión parcial** a partir de la función parcial k-ádica g (o del número natural a si $k = 0$) y la función parcial $k + 2$-ádica h si f está definida exactamente para aquellos naturales $a_1, \dots, a_k, n$ tales que

$g(a_1, \dots, a_k)$ está definido si $k = 0$

$f(u, a_1, \dots, a_k)$ está definido para todo $u < n$,

$h(u, f(u, a_1, \dots, a_k), a_1, \dots, a_k)$ está definido para todo $u < n$,

y se cumple

$$f(0, a_1, \dots, a_k) = g(a_1, \dots, a_k)$$

$$f(n + 1, a_1, \dots, a_k) = h(u, f(u, a_1, \dots, a_k), a_1, \dots, a_k) \; si \; 0 \leq u < n$$

c) Una función parcial n-ádica f está definida por **minimización parcial** a partir de una función parcial $n + 1$-ádica g si f está definida exactamente para aquellos naturales $a_1, \dots, a_n$ tales que existe un natural m que cumple

1) Si $k \leq m$ entonces g está definida para $a_1, \dots, a_n, k$

2) $g(a_1, \dots, a_n, m) = 0$ y se cumple

$$f(a_1, \dots, a_n) = \mu m g(a_1, \dots, a_n, m) = 0$$

Una vez nombrados los procesos de definición ahora tenemos la definición formal:

Definición 4.9: Una función parcial f es **recursiva parcial** si hay una sucesión de funciones $f_1, \dots, f_n$ tales que f_n es f y cada f_i es recursiva elemental o está definida por composición, recursión o minimización parcial a partir de funciones anteriores de la sucesión.

Obviamente, toda función recursiva es recursiva parcial.

§5 Máquina de Turing y la Tesis de Church-Turing

El argumento de Turing para probar que las funciones recursivas coinciden con las funciones calculables mediante un algoritmo se basa en el concepto de máquina de Turing. Esta solo pueden reconocer conjuntos recursivamente enumerables.

- *Máquina de Turing*

Una máquina de Turing es un concepto abstracto de la misma naturaleza que una teoría axiomática, es decir, un sistema conceptual que fundamenta una serie de afirmaciones objetivas, para las cuáles veremos una serie de definiciones.

Una máquina de Turing consta de una cinta infinita dividida en infinitas casillas contiguas infinitamente prolongable tanto a izquierda como a derecha. Cada casilla puede estar en blanco o tener impreso un *signo* de entre los de una lista finita que llamaremos *alfabeto*: $s_1, \dots, s_j$ $(j \geq 1)$ fija para cada máquina particular. Escribiremos s_0 para nombrar al "blanco" (o no escribiremos nada) y así la situación posible de una casilla será una de entre $s_0, \dots, s_j$. En cualquier momento la cinta tendrá un número finito de casillas impresas (con signos distintos de s_0). El estado de la cinta en un momento dado lo llamaremos *situación*.

	s_1			s_2	s_2	s_3		s_1	s_1			s_4	s_1		

En cada instante la máquina se encontrará en un *estado* de entre un número finito posible de ellos $q_0, \dots, q_k$ $(k \geq 1)$ fijo para cada máquina particular. A q_1 le llamaremos *estado inicial*, es el estado en que se encuentra la máquina cuando empieza a funcionar. El estado de la máquina y el signo escrutado determinan la *configuración* de la máquina en un instante dado. Entonces una máquina de Turing se compone de una función que a cada configuración activa (s_a, q_b) le asigna una terna (s_c, M, q_d), donde s_c , M y q_d son, respectivamente, el signo impreso, el movimiento realizado I, D o C (izquierda, derecha o centro) y el estado al que se pasa, todo esto cuando la configuración es (s_a, q_b). A esta función se le llama *programa* de la máquina.

Llamaremos *representación* de los números $a_1, \dots, a_n$ a la situación que consta de n secuencias de $a_i + 1$ signos s consecutivos cada una, separadas por un blanco. Llamaremos *representación normal* o *posición normal* de los naturales $a_1, \dots, a_n$ a la representación de $a_1, \dots, a_n$ cuando la casilla escrutada es la última casilla impresa de a_n.

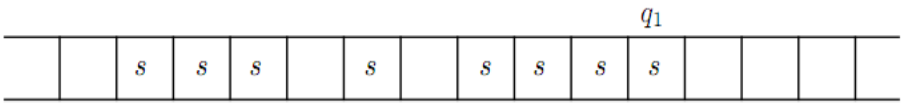
Definición 5.1: Una máquina de Turing M *computa* la función parcial n-ádica f si cuando M comienza con los números $a_1, \dots, a_n$ en posición normal y el resto de la cinta en blanco, termina con la representación normal de

$$a_1, \dots, a_n, f(a_1, \dots, a_n)$$

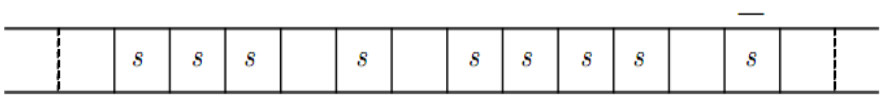
en el caso de que $f(a_1, \dots, a_n)$ esté definido. Si $f(a_1, \dots, a_n)$ no está definido entonces M no se detiene.

Una función recursiva parcial es **computable** si hay una máquina de Turing que la computa. Una máquina de Turing M computa la función parcial n-ádica f.

Ejemplo: Si $f(2, 0, 3) = 0$ y M computa f, cuando M comienza con



y termina con: (el guión sobre s indica que está en posición normal)



- *Tesis de Church-Turing*

Sabemos que toda función recursiva es calculable mediante un algoritmo. El siguiente teorema explicita este hecho.

Teorema 5.2: *Toda función recursiva parcial es computable*.

Demostración:

Por inducción sobre el número r de funciones de una sucesión que defina a f. Si $r = 1$ se trata de una función recursiva elemental.

Supongamos ahora que f se define en r pasos y que todas las funciones definibles en menos de r pasos son computables (hipótesis inductiva). Distinguimos tres casos, según que f se defina por composición, recursión o minimización a partir de funciones anteriores (que por hipótesis de inducción serán computables).

Caso *a)* La función f está definida por composición a partir de las funciones g y h:

$f(a_1, \dots, a_n) = g(h_1(a_1, \dots, a_n), \dots, h_m(a_1, \dots, a_n))$, donde las funciones g y h_i son computables por máquinas M_g y M_{h_i} respectivamente (hipótesis de inducción).

Como ya dijimos una función recursiva parcial es computable si hay una máquina de Turing que la computa. Entonces, veamos que la función f es computada por la máquina:

$$M_f = K_n M_{h_1} I_{n+1}^n M_{h_2} I_{n+1}^n \dots I_{n+1}^n M_{h_m} I_{(m-1)(n+1)+1} I_{(m-2)(n+1)+2} \dots I_{0(n+1)+m} M_g LB$$

Veamos en que consisten cada una de las máquinas con las que se compone M_f.

Supongamos definido $f(a_1, \dots, a_n)$. Si M_f empieza con $a_1, \dots, \overline{a_n}$, en primer lugar K_n copia $a_1, \dots, a_n$ con un vacío en medio: $a_1, \dots, a_n, \ , a_1, \dots, \overline{a_n}$

Luego M_{h_1} calcula $h_1(a_1, \dots, a_n)$:

$$a_1, \dots, a_n, \ , a_1, \dots, a_n, \overline{h_1(a_1, \dots, a_n)}$$

Ahora I_{n+1}^n copia $a_1, \dots, a_n$ y M_{h_2} calcula $h_2(a_1, \dots, a_n)$:

$$a_1, \dots, a_n, \ , a_1, \dots, a_n, h_1(a_1, \dots, a_n), a_1, \dots, a_n, \overline{h_2(a_1, \dots, a_n)}$$

Tras haber actuado M_{h_m} tenemos

$$a_1, \dots, a_n, \ , a_1, \dots, a_n, h_1(a_1, \dots, a_n), \dots, a_1, \dots, a_n, \overline{h_m(a_1, \dots, a_n)}$$

Luego las máquinas $I_{(m-2)(n+1)+2} \dots I_{0(n+1)+m}$ copian $h_1(a_1, \dots, a_n), \dots, h_m(a_1, \dots, a_n)$ y entonces M_g calcula la imagen de estos números por g, o sea, calcula $f(a_1, \dots, a_n)$. La situación de la cinta es entonces:

$$a_1, \dots, a_n, \ , x_1, \dots, x_r, \overline{f(a_1, \dots, a_n)}$$

La máquina L borra $x_1, \dots, x_r$ y B borra el vacío intermedio, hasta quedar $a_1, \dots, a_n, \overline{f(a_1, \dots, a_n)}$

Si $f(a_1, \dots, a_n)$ no está definida, entonces no lo está alguna de las funciones $g, h_1, \dots, h_n$, por lo que la máquina correspondiente no se para y M_f tampoco.∴

Caso *b)* La función f está definida por recurrencia a partir de las funciones g y h, es decir:

$$f(0, a_2, \dots, a_n) = g(a_2, \dots, a_n)$$

$$f(a+1, a_2, \dots, a_n) = h(a, f(a, a_2, \dots, a_k), a_2, \dots, a_n).$$

Por hipótesis de inducción existen máquinas M_g y M_h que computan a g y h respectivamente. Razonando de forma similar al caso anterior es fácil ver que la función f es computada por la máquina:

$$M_f = K_n M_g I_{n+1} E \left[\begin{array}{l} I_2 LB \\ CI_3 I_{n+3}^{n-1} M_h I_{n+3} FE \left[\begin{array}{l} I_2 LB \\ I_{n+3} A \end{array} \right. \end{array} \right.$$

Observación: Detallaremos el comportamiento de las máquinas A, C, E y F ya que en el caso anterior no estaban incluidas.

A: imprime sobre un espacio vacío.

C: Cuando empieza con un número en posición normal va dos lugares a la derecha e imprime.

E: Cuando empieza con un número en posición normal toma la salida 0_1 o 0_2 según sea 0 o distinto de 0 y termina en posición normal.

F: Cuando comienza en una casilla impresa, borra y va una casilla a la izquierda.

Caso *c)* La función f está definida por minimización a partir de las funciones g y h:

$$f(a_1, \dots, a_n) = \mu x g(a_1, \dots, a_n, x) = 0.$$

Por hipótesis de inducción existe una máquina M_g que computa a g. Entonces la función f es computada por la máquina:

$$M_f = K_n C M_g E \left[\begin{array}{l} I_2 LB \\ I_{n+2}^{n+1} A \end{array} \right.$$

De este modo, para cada función recursiva parcial f sabemos construir explícitamente una máquina de Turing que la computa. Por lo tanto toda función recursiva parcial es computable.

§6 Teorema de Matijasevic y solución al décimo problema de Hilbert

A lo largo de todo el trabajo hemos demostrado algunas propiedades y teoremas que son importantes para la demostración del teorema de Matijasevic. En primer lugar, en la sección 4 demostramos que la función exponencial es recursiva y en la sección 3 que es diofántica (Recordemos que una ecuación diofántica es una ecuación polinómica, por este motivo hemos demostrado el carácter diofántico de la función exponencial). Este es un hecho crucial para resolver el décimo problema de Hilbert, así como también que toda función recursiva es computable y que no todo conjunto recursivamente enumerable es recursivo. Este hueco entre los conjuntos es lo que hace posible demostrar la insolubilidad algorítmica. Ahora veremos la razón. Lo que será demostrado aquí es inexistencia de solución del décimo problema de Hilbert, es decir la no existencia de un algoritmo de solución sobre números enteros para una ecuación diofántica.

- *Teorema de Matijasevic*

El Teorema de Matijasevic afirma que todo conjunto recursivamente enumerable es diofántico. Para escribir este enunciado en forma simbólica supongamos que $A(a_1, \dots, a_m)$ es un conjunto r.e. y usando la definición 1.1 de conjuntos diofánticos queda:

Teorema 6.1: Todo conjunto r.e. $A(a_1, \dots, a_m)$ puede ser representado en la siguiente forma:

$$A(a_1, \dots, a_m) \Leftrightarrow (\exists x_1, \dots, x_n)[P(a_1, \dots, a_m, x_1, \dots, x_n) = 0]$$

Como hemos definido en la sección 4 un conjunto es r.e. si coincide con el rango exacto de una función recursiva (Definición 4.7). Además, una función recursiva es computable y esta tiene como imagen al conjunto r.e. Entonces si tenemos como hipótesis que el rango de una función recursiva f coincide con el conjunto A, por lo tanto A es r.e. el teorema anterior se reduce a probar el siguiente teorema:

Teorema 6.1.1: Toda función recursiva es diofántica.

Demostración:

En primer lugar observamos que las funciones recursivas elementales son claramente diofánticas aplicando la definición 1.2:

$$y = c(x) \Leftrightarrow y = 0$$

$$y = s(x) \Leftrightarrow y = x + 1$$

$$y = p_i^k(x_1, \dots, x_k) \Leftrightarrow y = x_i$$

Como ya dijimos, las funciones recursivas son las que pueden obtenerse a partir de las elementales mediante la aplicación de un número finito de los procesos de definición los cuales son: composición, recursión y minimización. Como las funciones recursivas elementales son diofánticas debemos demostrar que las funciones recursivas que se obtienen a partir de estas también son diofánticas.

Ahora veamos, que las funciones recursivas obtenidas mediante estos procesos son diofánticas.

a) La composición de funciones diofánticas es diofántica:

$$h(x_1, \dots, x_n) = f\big(g_1(x_1, \dots, x_n), \dots , g_m(x_1, \dots, x_n)\big)$$

Entonces

$$y = h(x_1, \dots, x_n) \leftrightarrow \forall y_1, \dots, y_m (y_1 = g_1(x_1, \dots, x_n) \wedge \dots \dots . \wedge y_m = g_m(x_1, \dots, x_n) \quad \wedge \quad y = h(y_1, \dots, y_m)).$$

Claramente h es diofántica.

b) Veamos ahora que si

$$h(x_1, \dots, x_n, 0) = f(x_1, \dots, x_n),$$

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

y las funciones f y g son diofánticas (elementales), entonces h también lo es. En efecto,

$$y = h(x_1, \dots, x_n, z) \leftrightarrow \forall u \in \mathbb{N}(\forall v \in \mathbb{N}(v = S(0, n) \wedge v = f(x_1, \dots, x_n))$$

$$\wedge \exists t \in \mathbb{N}(t \leq z \rightarrow t = z \vee \forall v \in \mathbb{N}(v = S(t + 1, u)$$

$$\wedge v = g(t, S(t, u), x_1, \dots, x_n))) \ \wedge y = S(z, u)),$$

Esto prueba que h es diofántica, ya que cumple la definición.

El caso $n = 0$ es similar:

$$y = h(x, z) \leftrightarrow \forall u \in \mathbb{N}(\forall v \in \mathbb{N}(v = S(0, n)$$

$$\wedge\, v = f(x)) \wedge \exists t \in \mathbb{N}(t \leq z \rightarrow t = z \vee \forall v \in \mathbb{N}(v = S(t+1, u)$$

$$\wedge\, v = g(t, S(t,u), x))) \;\wedge y = S(z,u)),$$

c) Por último, si $h(x_1, \dots, x_n) = \mu y f(x_1, \dots, x_n, y) = 0$ y f es diofántica (función elemental), entonces h también lo es, ya que

$$y = h(x_1, \dots, x_n) \leftrightarrow \forall z \in \mathbb{N}(z = f(x_1, \dots, x_n, y) \wedge z = 0)$$

$$\wedge\, \exists t \in \mathbb{N}(t \leq y \rightarrow t = y \;\vee \forall u \in \mathbb{N}(u = f(x_1, \dots, x_n, t) \wedge u > 0)))$$

Esto último prueba que h es diofántica, ya que cumple la definición.

Como las funciones recursivas obtenidas mediante composición, recursión y minimización a partir de las elementales también son diofánticas. Por lo tanto, toda función recursiva es diofántica. Con esto queda demostrado el teorema 6.1.1. y por las explicaciones dadas más arriba también el teorema 6.1.

Entonces, que una función recursiva sea diofántica implica que todo conjunto r.e. es diofántico ya que la imagen de esa función recursiva es el conjunto A, el cual es r.e.

- *Solución negativa al décimo problema de Hilbert.*

Recordemos que el décimo problema de Hilbert pedía un procedimiento mecánico que determinara la solubilidad o insolubilidad de una ecuación diofántica en los enteros. Para finalmente probar que este problema no tiene solución, primero demostraremos un lema previo para el cual necesitamos una función y un conjunto definidos como sigue.

Retomando los conceptos vistos en la sección 5: Sea M una máquina de Turing que devuelva el mayor número de registro $R_i(i)$ y se detenga. Aquí llamaremos registro a lo que definimos en la sección anterior como signo: $s_1, \dots, s_j$ $(j \geq 1)$ para no generar ambigüedad en el lenguaje. Entonces, sea $R(\ell)$ el mayor valor generado por este proceso, es decir por medio de una máquina con ℓ instrucciones como algoritmo y con la configuración inicial: cero en todos sus registros. Por ejemplo $R(1) = 1$ y $R(2) = 2$. En la primera el algoritmo es que se incremente 1 a $R_1 = 0$ y en la segunda dos veces este procedimiento.

$R(\ell)$ es una función creciente en ℓ. Esto es, $R(\ell) < R(\ell + 1)$.

La función $R(\ell)$ es una función recursiva ya que es computable mediante una máquina de Turing y además está definida por composición de funciones anteriores.

Consideremos ahora el siguiente conjunto:

$$S = \{k: k \in \mathbb{N} \wedge k \leq R(\ell)\}$$

Donde k son los naturales que va generando la función recursiva $R(\ell)$ mediante la máquina de Turing M.

El conjunto S es r.e. ya que es la imagen de la función recursiva $R(\ell)$ y además

$$S = rang\big(R(\ell)\big) = \{R(1), R(2), .., R(\ell)\}\,.$$

Lema 6.2: Sea f cualquier función calculable. Entonces, para ℓ suficientemente grande, $f(\ell) < R(\ell)$.

Demostración:

Asumamos que la función calculable f es una función creciente. Por ser calculable existe una máquina de Turing N que calcule la función f. Supongamos que N tiene c instrucciones como algoritmo. Sea F la máquina de Turing obtenida al adherir la instrucción "$sumar\ 1$" al final del algoritmo de N. Entonces F tiene $c + 1$ instrucciones como algoritmo y calcula el valor $f(x) + 1$.

Ahora consideremos una máquina de Turing D con 5 instrucciones como algoritmo y esta tiene la propiedad que comienza con x en el registro R_2, es decir $R_2 = x$ y cero en R_1y que termine con $R_1 = 2x$ y se detiene. Por otro parte para cada x, sea M_x una máquina de Turing con la propiedad que cuando comience el cálculo, tenga $R_2 = 0$ y al terminar $R_2 = x$. Es decir, tiene x instrucciones como algoritmo.

Si consideramos la máquina $F(D(M_x))$ tiene $c + 1 + 5 + x = x + 6 + c$ instrucciones como algoritmo. Por ser $F(D(M_x))$ una composición de algoritmos esta máquina con sus registros en cero al comenzar produce el valor $F\big(D(x)\big) = F(2x) = f(2x) + 1$ y se detiene. Así el mayor valor producido por esta máquina con $x + 6 + c$ instrucciones como algoritmo es $R(x + 6 + c) = f(2x) + 1$. Donde R es la función recursiva definida más arriba y $\ell = x + 6 + c$. Luego para cada x

$$f(2x) < R(x + 6 + c)$$

Cuando $x \geq 6 + c$,

entonces $x + x \geq x + 6 + c \implies 2x \geq x + 6 + c$.

Como f es creciente tenemos que $f(2x) \geq f(x + 6 + c)$.

Sea $\ell = x + 6 + c$, entonces $f(\ell) = f(x + 6 + c) \leq f(2x) < R(x + 6 + c) = R(\ell)$

Podemos establecer que $R(x + 6 + c) = R(\ell)$ por definición de la función R ya que es el mayor valor producido por la máquina $F(D(M_x))$ con $x + 6 + c$ instrucciones.

Por lo tanto, $f(\ell) < R(\ell)$. El lema ha sido probado.

Observación: En toda la prueba anterior se entiende como "máquina" no como una máquina real sino como un conjunto de instrucciones que conforman el algoritmo de función calculable.

Teorema 6.3: No existe un algoritmo que resuelva el décimo problema de Hilbert.

Demostración:

Supongamos que existe un algoritmo que resuelva el décimo problema de Hilbert. Es decir, supongamos que existe un procedimiento mecánico que en un número finito de pasos permita decidir si una ecuación diofántica tiene soluciones enteras o no. Entonces, teniendo la función recursiva R definida en este apartado, la cual es calculable por la tesis de Church-Turing, por la cual se obtiene el conjunto S r.e. que es diofántico por el teorema 6.1, podemos aplicar el lema 6.2 y tendríamos ℓ suficientemente grande tal que $R(\ell) < R(\ell)$. ¡Absurdo!.

Así el décimo problema de Hilbert no tiene solución ya que si R es recursiva (calculable) entonces es diofántica por el teorema 6.1.1 y al obtener un absurdo del lema 6.2 significa que no existe un algoritmo que permita decidir si una ecuación diofántica tiene solución o no.

Más aún, según la definición de máquina de Turing M se detiene en el caso de que $f(a_1, \dots, a_n)$ esté definido terminando con la representación de todos los valores obtenidos $a_1, \dots, a_n, f(a_1, \dots, a_n)$, este es el conjunto diofántico. Si $f(a_1, \dots, a_n)$ no está definido entonces M no se detiene. Lo cual indica que la ecuación diofántica no tiene solución y según lo que obtuvimos de aplicar el lema 6.2 no puede ser calculado por una máquina de Turing una función recursiva en la que sí está definido $f(a_1, \dots, a_n)$. De aquí proviene el absurdo.

Con la demostración de este teorema se completa el propósito de este trabajo.

Conclusión

En el décimo problema de Hilbert se pide determinar un procedimiento mecánico que determine en un número finito de pasos si una ecuación diofántica tiene soluciones enteras o no. En realidad lo que pedía Hilbert era un algoritmo que solucione el décimo problema.

Hilbert estaba interesado en una solución positiva del problema. Existen varias versiones que explican el interés de Hilbert:

- Deseaba extender la teoría de formas cuadráticas indefinidamente a más variables.
- El pensaba que era posible eliminar los detalles y la prueba abstracta en la solución de problemas (solucionar el *Entscheidungsproblem* de Hilbert).
- Fue una manifestación de su fe en la habilidad de los matemáticos para resolver todos los problemas matemáticos que el encontró y no había solucionado.

Inmediatamente después de la demostración de Matijasevic surgieron nuevas pruebas usando sucesiones de soluciones de la ecuación de Pell, hechas por los matemáticos Davis, Chudnosky y Kosovskii.

Debido a la insolubilidad del décimo problema de Hilbert se produjeron consecuencias importantes. Una de ellas es que debe existir un polinomio que genere todos los números primos. Ya que posteriormente se demostró un teorema que establece que todo conjunto r.e. de números naturales coincide con los valores no negativos de cierto polinomio en Q y se consideró el conjunto de los números primos el cual es r.e. En consecuencia, existe un polinomio explícito de grado 25 en 26 variables.

Otra implicación muy importante de la solución negativa del décimo problema de Hilbert es el teorema de incompletitud de Gödel demostrado en 1931.

Bibliografía

Libros

- Ivorra Castillo, Carlos. *Lógica y teoría de conjuntos*. Capítulos V y VII
- Gray, Jeremy. *El reto de Hilbert*. Año 2003. Pág 242-252.
- Torreti, Roberto. *El paraíso de Cantor: La tradición conjuntista*. Santiago de Chile. Año 1998. Pág 359-419.
- Gil Alegre, Carmen; Martínez Pastor, Ana; Pedraza Aguilera, María del Carmen. *Problemas de matemática discreta*. Universidad de Valencia. Pág 425-427.
- Ferrando, J.C.; Gregori, V. Matemática discreta. Editorial Reverté. Año 1995. Pág 178-194.

Artículos

- Martin Davis. *Hilbert's tenth problem is unsolvable.* American Mathematical Monthly 80 (1973). Pág 233–269.
- *Proof of recursive unsolvability of Hilbert's tenth problem.* American Mathematical Monthly 89 (1991). Pág 689–709.
- Fariña, Juan Carlos. *Los 23 problemas de Hilbert*. Los matemáticos del siglo XX. Pág 25-28.
- Castaño, Enrique Gallego. *Técnicas de demostración de indecibilidad e inseparabilidad en teorías formales*. Tesis doctoral. Madrid, Mayo de 2001. Pág 11-36.
- Parra Machío, Rafael. *La ecuación de Pell: origen de la ecuación*. http://hojamat.es/parra/pell.pdf.
- Pérez, Sonia Alanya. *Ecuación de Pell y unidades en el anillo de enteros de los cuerpos cuadráticos*. Trabajo monográfico. Universidad nacional mayor de san marcos. Lima, Perú. Año 2004.
- Vélez Marulanda, José Alberto. El *décimo problema de Hilbert*. Trabajo de grado. Universidad Nacional de Colombia. Año 2001.