Décimo Problema de Hilbert, Curvas Elípticas y Algunas Extensiones

por

Danny Arlen de Jesús Gómez Ramírez

Trabajo presentado como requisito parcial
para optar al Título de

Magister en Matemáticas

Juan Diego Vélez Caicedo

Universidad Nacional de Colombia
Sede Medellín

Facultad de Ciencias

Escuela de Matemáticas

Marzo 2007

Resumen

En este trabajo presentamos una prueba completa de la insolubilidad algorítmica del décimo problema de Hilbert. Además, mostramos tres extensiones del mismo, a otros anillos de interés. Finalmente, exponemos la situación actual del décimo problema de Hilbert sobre los números racionales.

Contenido

Agradecimientos

Quisiera agreceder a los profesores Juan Diego Vélez, Carlos Mario Parra, Carlos Videla, Alf Onshuus y Carlos Cadavid por su colaboración en la realización de este trabajo. Además, a mis compañeros de maestría, a Ingrid Gonzalez, a mis padres, a Dios, al profesor Jairo Gómez. Finalmente, agadecimientos muy especiales a Yoe Alexander Herrera, por su ayuda en la edición.

Introducción

Desde la época de Diofanto de Alejandría los matemáticos se han interesado por resolver ecuaciones diofantinas, es decir, ecuaciones de la forma $D(x_1, x_2, \ldots, x_n) = 0$, donde D es un polinomio en n variables, con coeficientes en los números enteros. Resolver la ecuación significa encontrar valores entereos en las variables $x_1, x_2, \ldots, x_n$ de modo tal que la ecuación $D = 0$ se satisfaga. Esta área de las matemáticas, llamada Análisis Diofantino, es extremedamente complicada y utiliza en sus métodos la gran mayoría de las ramas más importantes de las matemáticas modernas como la geometría algébraica, el análisis complejo, el análisis armónico y la topología, entre otras. Una cuestión más general y en principio menos compleja que la de resolver o encontrar las soluciones de una ecuación diofantina, es la de decidir si ésta tiene o no soluciones enteras, sin preocuparse por mostrar explícitamente dichas soluciones. Esta pregunta fue la que motivó a Hilbert a incluir en sus 23 problemas el siguiente interrogante: ¿existe un "método" (algoritmo) para determinar si una ecuación diofantina arbitraria tiene o no soluciones enteras? Esta pregunta era bastante ambiciosa y Hilbert la planteó de manera afirmativa, es decir, Hilbert creía que existía un método universal que permitía decidir la solubilidad de ecuaciones diofantinas en los números enteros. Sin embargo, en 1970, Yuri Matiyasevich demostró el último hecho que faltaba para probar que la pregunta planteada por Hilbert (actualmente conocida como el décimo problema de Hilbert) era insoluble algorítmicamente. De hecho, este resultado fue probado en un trabajo conjunto de los matemáticos Martin Davis, Yuri Matiyasevich, Hilary Putnam y Julia Robinson. Desde entonces el interés se ha centrado en extender este resultado a otros anillos diferentes de $\mathbb{Z}$, entre estos está el problema más importante de esta área: saber si existe o no un algóritmo para decidir si una determinada ecuación diofantina tiene solución en los números racionales. Esta monografía está dividida en tres partes. En la primera parte se expone la demostración más corta y simplificada de la insolubilidad del décimo problema de Hilbert. También se exponen allí varias consecuencias sorprendentes de este hecho. En la segunda parte se prueban resultados análogos al décimo problema de Hilbert sobre anillos más generales y se muestra una aplicación de la teoría de las curvas elípticas a este problema. En la tercera y última parte, mostraremos los avances que se han realizado hasta el momento sobre el décimo problema de Hilbert en los números racionales.

Se presenta además una tabla que resume el estatus del problema de Hilbert en otros anillos de interés. Se espera que este trabajo sirva como introducción a las técnicas más básicas en esta bellísima área de las matemáticas.

Capítulo 1

Insolubilidad del décimo problema de Hilbert

1.1 Introducción

En su famosa conferencia dictada durante el Segundo Congreso Internacional de Matemáticas en Paris, en 1990, el matemático alemán David Hilbert propuso 23 problemas que marcarían, en su opinión, el desarrollo de las matemáticas del siglo XX. La formulación del décimo problema es tan corta que se puede reproducir aquí literalmente:

ENTSCHEIDUNG DER LÖSBARKEIT EINER DIOPHANTISCHEN GLEICHUNG

Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen ralionalen Zahlkoefficienten sei vorgelegti man soll ein Verfahren angebe, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden läβt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

Una ecuación diofantina es una ecuación de la forma

$$P\left(x_1, x_2, \ldots, x_n\right) = 0, \tag{1.1}$$

donde P es un polinomio con coeficientes en los números enteros. El décimo problema de Hilbert pide encontrar un "método" por medio del cual se pueda determinar, en un número finito de operaciones, si una ecuación diofantina arbitraria es soluble en los números enteros. En el contexto en el que problema fue planteado, la palabra "método", indicaba un procedimiento mecánico general, determinado por una lista de instrucciones, y que no dependiera de la ecuación diofantina particular que se analizara. En lenguaje moderno, se pide encontrar un *algoritmo* que decida la solubilidad de ecuaciones diofantinas en $\mathbb{Z}$.

Durante el periodo comprendido entre la vida de Diofanto (año 300 a.c.) y 1900, los teóricos de números habían encontrado soluciones enteras para un gran número de ecuaciones diofantinas particulares y habían demostrado que otro gran número de ellas eran insolubles. Sin embargo, nadie conocía *un método general* que permitiese determinar si cualquier ecuación que se analizara tenía o no solución, razón que llevo a Hilbert a plantear el problema en esta generalidad, creyendo que tal método posiblemente pudiera desarrollarse durante el siglo que apenas

comenzaba. A lo largo de más de 50 años muchos matemáticos trataron de encontrar dicho método universal pero fracasaron. Debido a esto y a la formalización de la noción de algoritmo (Gödel, Turing, Post, Church entre otros) se comenzó a pensar en cómo demostrar la insolubilidad del décimo problema de Hilbert ($H10\,(\mathbb{Z})$ para abreviar). Cabe citar las palabras de Emil Post: "El décimo problema de Hilbert pide una prueba de insolubilidad", que pronunció después de demostrar, junto con Andrei Markov, que el problema de la palabra para semigrupos era indecidible. Inspirado en estas palabras, Martin Davis (estudiante de Emil Post) comenzó su larga ofensiva contra $H10\,(\mathbb{Z})$. Poco tiempo después, Davis estableció una hipótesis que implicaría la insolubilidad de $H10\,(\mathbb{Z})$. Finalmente, en 1970 Yuri Matiyasevich, basado en los trabajas de M. Davis, H. Putnam y J. Robinson, logró demostrar la hipótesis de Davis, y por consiguiente, la insolubilidad de $H10\,(\mathbb{Z})$.

En este capítulo mostraremos la prueba más corta, conocida hasta la fecha, de la insolubilidad de $H10\,(\mathbb{Z})$. En esta demostración están todas las simplificaciones que fueron encontradas desde que el problema fue resuelto por Y. Matiyasevich [12]. Nos basaremos en un trabajo conjunto entre el último autor y J. P. Jones [9].

$H10\,(\mathbb{Z})$, es lo que actualmente se conoce como un problema de decisión, es decir, un problema que consta de infinitos subproblemas, cada uno de los cuales requiere una respuesta afirmativa o negativa. En nuestro caso particular cada subproblema es representado por una ecuación diofantina específica, a la cual damos una respuesta afirmativa o negativa, dependiendo de la solubilidad o insolubilidad de la ecuación en los números enteros. Por razones técnicas resulta más simple analizar el décimo problema de Hilbert en los números naturales ($H10\,(\mathbb{N})$), con lo cual no se pierde generalidad, como veremos enseguida. Sin embargo, para ecuaciones particulares estos dos problemas pueden ser bastante diferentes. Por ejemplo, la ecuación

$$(x+1)^3 + (y+1)^3 = (z+1)^3 \tag{1.2}$$

tiene, de manera trivial, infinitas soluciones enteras de la forma $x = z$ y $y = -1$. Pero, la no existencia de soluciones en los naturales para esta ecuación es un hecho nada trivial (caso particular del último teorema de Fermat).

No obstante, si consideramos $H10\,(\mathbb{Z})$ y $H10\,(\mathbb{N})$ como problemas de decisión ambos resultan ser equivalentes. En efecto, sea

$$P\,(x_1, x_2, \ldots, x_n) = 0 \tag{1.3}$$

una ecuación diofantina arbitraria. Supongamos que estamos buscando soluciones $x_1, x_2, \ldots, x_n \in \mathbb{Z}$. Entonces, si consideramos la ecuación

$$P\,(y_1 - z_1, y_2 - z_2, \ldots, y_n - z_n) = 0 \tag{1.4}$$

en las variables $y_1, z_1, y_2, z_2, \ldots, y_n, z_n$, es claro que la ecuación (1.3) tiene soluciones en $\mathbb{Z}$, si y sólo si, la ecuación (1.4) tiene solución en $\mathbb{N}$, ya que cualquier número entero se puede expresar como la diferencia de dos números naturales. De este modo, si existiera un algoritmo para resolver $H10\,(\mathbb{N})$, entonces existiría un algoritmo para decidir $H10\,(\mathbb{Z})$. La reducción en el otro sentido es menos evidente, pero también es cierta: en virtud del *teorema de Lagrange*, que establece que todo número natural es la suma de cuatro cuadrados. Usando este resultado tenemos que

$$(\exists x_1, x_2, \ldots, x_n \in \mathbb{N})\,[P\,(x_1, x_2, \ldots, x_n) = 0] \Leftrightarrow \tag{1.5}$$

$$(\exists a_1, b_1, c_1, d_1, \ldots, a_n, b_n, c_n, d_n \in \mathbb{Z})$$

$$\left[P\left(a_1^2 + b_1^2 + c_1^2 + d_1^2, \ldots, a_n^2 + b_n^2 + c_n^2 + d_n^2\right) = 0\right] \tag{1.6}$$

Así, la solubilidad de $H10\,(\mathbb{N})$ se reduce a la solubilidad de $H10\,(\mathbb{Z})$. En conclusión, $H10\,(\mathbb{Z})$ *es insoluble si y sólo si* $H10\,(\mathbb{N})$ *es insoluble.* En este capítulo probaremos que $H10\,(\mathbb{N})$ es insoluble. Al afirmar que probaremos la insolubilidad algorítmica de $H10\,(\mathbb{N})$, estamos usando implícitamente la bien conocida *hipótesis de Church-Turing.* Esta hipótesis establece que *cada procedimiento puramente mecánico puede ser computado por una máquina de Turing.* Existen muchos modelos formales para describir de manera rigurosa la noción de algoritmo. Entre ellos están las máquinas de Turing, las máquinas registradoras y los algoritmos de Markov. Todas estas formalizaciones se han demostrado ser equivalentes en términos de lo que pueden computar. La noción de máquina registradora será la que usaremos en este capítulo, ya que permite describir, de modo más simple, muchas propiedades aritméticas de los números naturales.

Un conjunto (ó relación) $S \subseteq \mathbb{N}^n$ se llama *recursivamente enumerable o listable* (r.e) si puede ser computado por una máquina registradora o máquina de Turing. Una función f, definida en un conjunto de n-tuplas de naturales y con valores en m-tuplas de naturales, es *recursiva*, si su gráfica es un conjunto listable. Un conjunto de n-tuplas de naturales se llama *recursivo*, si su función característica es recursiva. Claramente, si un conjunto es recursivo, entonces es listable. Lo que no es trivial, es el hecho de que existan conjuntos listables que no son recursivos, como por ejemplo, el *conjunto de parada*, que se define como el conjunto de tuplas de números naturales, (n, m), tales que la n-ésima máquina de Turing (fijando una gödelización, esto es, una enumeración efectiva de las máquinas de Turing) se detiene al evaluar n.

El teorema central de este capítulo, del cual se desprende la insolubilidad de $H10\,(\mathbb{N})$ y una gran cantidad de corolarios importantes, es el siguiente:

Teorema 1.1.1 *Cada relación listable (r.e.)* $A\,(a_1, a_2, \ldots, a_m)$ *puede ser representada en la forma*

$$A\,(a_1, a_2, \ldots, a_m) \Leftrightarrow (\exists x_1, \ldots, x_n \in \mathbb{N})\,[P\,(a_1, a_2, \ldots, a_m, x_1, \ldots, x_n) = 0] \tag{1.7}$$

donde $P(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n)$ *es un polinomio con coeficientes enteros.*

Es decir, el teorema afirma que para cada conjunto r.e. de m-tuplas $A(a_1, a_2, \ldots, a_m)$, existe un polinomio diofantino

$$P(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n)$$

(que depende de A), de tal manera que para saber si una m-tupla de números naturales pertenece a A, basta saber si la ecuación diofantina

$$P(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n) = 0$$

tiene soluciones en las variables $x_1, x_2, \ldots, x_n \in \mathbb{N}$. El Teorema 1.1.1 se conocía como la hipótesis de Martin Davis y actualmente se conoce como el *teorema DPRM (Davis-Putnam-Robinson-Matiyasevich).*

La insolubilidad de $H10(\mathbb{N})$ se sigue inmeditamente del Teorema 1.1.1 ya que si existiera algún algoritmo para decidir $H10(\mathbb{N})$, se tendría, para cada conjunto A, una representación como en (1.6). Luego, para cada m-tupla $(a_1, a_2, \ldots, a_m)$ se podría decidir algorítmicamente si existen $x_1, x_2, \ldots, x_n \in \mathbb{N}$ tales que

$$P(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n) = 0,$$

o lo que es equivalente, podríamos decidir si $(a_1, a_2, \ldots, a_m)$ pertenece o no al conjunto A. Esto significa que A sería un conjunto recursivo, lo cual es absurdo si tomamos a A como el conjunto de parada.

Éste ha sido el argumento estándar para demostrar que la hipótesis de Martin Davis implica la insolubilidad de $H10(\mathbb{N})$. Al final de este capítulo daremos una demostración adicinonal de esta implicación usando una idea de T. Rado. Vale la pena notar que el Teorema 1.1.1, independiente del décimo problema de Hilbert, describe una relación muy profunda entre un concepto puramente aritmético (conjunto diofantino, definido por el lado derecho de la Ecuación 1.5) y un concepto netamente lógico, como lo es el de conjunto listable. La demostración del Teorema 1.1.1 es, en muchos aspectos, constructiva, dado que permite construir en muchas situaciones, una representación diofantina para conjuntos tan fundamentales en teoría de números como el conjunto de los números primos.

1.2 Conjuntos diofantinos

Si $P(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n)$ es un polinomio diofantino (con coeficientes en $\mathbb{Z}$), entonces a las entradas de P las dividiremos por conveniencia en parámetros $a_1, a_2, \ldots, a_m$ y variables

$x_1, x_2, \ldots, x_n$. Todas las variables y parámetros varían en el conjunto de los números naturales $0, 1, 2, \ldots$En la teoría clásica de ecuaciones diofantinas se comienza con una ecuación diofantina particular y se busca describir el conjunto de sus soluciones. Nosotros, en cambio, estaremos interesados en el problema opuesto, o sea, dado un conjunto listable $A(a_1, a_2, \ldots, a_m)$ buscaremos un polinomio diofantino

$$P(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n)$$

que defina a A en el sentido de (1.6).

Definición 1.2.1 *Una relación $A(a_1, a_2, \ldots, a_m)$ es diofantina si existe un polinomio diofantino $P(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n)$ tal que para cada conjunto de valores $a_1, a_2, \ldots, a_m$ se cumple que*

$$A(a_1, a_2, \ldots, a_m) \Leftrightarrow (\exists x_1, x_2, \ldots, x_n)\left[P(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n) = 0\right] \tag{1.8}$$

Esta definición, en principio para relaciones, se puede extender naturalmente a funciones. En efecto, diremos que una función f es diofantina si su gráfica lo es. Si A y B son conjuntos diofantinos de m-tuplas definidos por polinomios

$$P_A(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n) \text{ y } P_B(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n),$$

respectivamente, entonces $A \cap B$ y $A \cup B$ son también conjuntos diofantinos. Esto es cierto debido a las siguientes equivalecias:

$$\begin{aligned} A \cup B(c_1, \ldots, c_m) \quad \Leftrightarrow \quad & (\exists x_1, \ldots, x_n, y_1, \ldots, y_s) \\ & \left[P_A(c_1, \ldots, c_m, x_1, \ldots, x_n)\, P_B(c_1, \ldots, c_m, y_1, \ldots, y_s) = 0\right], \end{aligned} \tag{1.9}$$

$$\begin{aligned} A \cap B(c_1, \ldots, c_m) \quad \Leftrightarrow \quad & (\exists x_1, \ldots, x_n, y_1, \ldots, y_s) \\ & \left[P_A^2(c_1, \ldots, c_m, x_1, \ldots, x_n) + P_B^2(c_1, \ldots, c_m, y_1, \ldots, y_s) = 0\right] \end{aligned} \tag{1.10}$$

A continuación daremos algunos ejemplos de funciones y relaciones diofantinas bastante conocidas que nos serán de gran utilidad a lo largo de este capítulo.

$$\begin{aligned} a &\leq b \Leftrightarrow (\exists x)\,[a + x = b] \\ a|b &\Leftrightarrow (\exists x)\,[ax = b] \\ a &\equiv b \,(\mathrm{mod}\, c) \Leftrightarrow (\exists x)\,[a = b + cx \vee a = b - cx] \end{aligned} \tag{1.11}$$

Otros ejemplos importantes son la relación de coprimalidad $a \perp b\,(\mathrm{mcd}\,(a,b) = 1)$, la función residuo, $r = \mathrm{res}(a,b)$ (el residuo de dividir a entre b) y la relación cociente, $q = \mathrm{cos}(a,b)$ (el cociente de dividir a entre b).

$$\begin{aligned} a &\perp b \Leftrightarrow (\exists x, y)\,[ax - by = 1 \vee ax - by = -1]\,, \\ r &= \mathrm{res}\,(a,b) \Leftrightarrow r \equiv a\,(\mathrm{mod}\, b) \wedge 0 \leq r < b, \\ q &= \mathrm{cos}\,(a,b) \Leftrightarrow 0 \leq a - qb < b. \end{aligned} \tag{1.12}$$

Usando estas relaciones, y las ecuaciones 1.9 y 1.10, mostraremos que una gran cantidad de relaciones que nos serán de utilidad son diofantinas. Ahora, el Teorema 1.1.1 afirma que la clase de todos los conjuntos listables coincide con la clase de todos los conjuntos diofantinos. Una de las direcciones del teorema es relativamente sencilla. Es decir, si $A\,(a_1, a_2, \ldots, a_m)$ es un conjunto diofantino, con presentación diofantina dada por la expresión 1.7, entonces uno puede enumerar efectivamente el conjunto de $n + m$-tuplas recorriendo en orden este conjunto y verificando si

$$P\,(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n) = 0,$$

para cada $n + m$-tupla $(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n)$. Nótese que si para una $m + n$-tupla $(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n)$ se verifica que

$$P\,(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_n) \neq 0,$$

entonces no podemos concluir que $P\,(a_1, a_2, \ldots, a_m) \notin A$, ya que podría existir otra n-tupla $(y_1, y_2, \ldots, y_n)$ que cumpla

$$P\,(a_1, a_2, \ldots, a_m, y_1, y_2, \ldots, y_n) = 0.$$

La otra implicación es la más difícil y de su prueba nos ocuparemos en el resto de este capítulo.

1.3 La ecuación de Pell

Por razones técnicas comenzaremos considerando la ecuación de Pell general, que es una ecuación de la forma

$$x^2 - dy^2 = 1, \tag{1.13}$$

donde d no es un cuadrado perfecto y x, y son variables desconocidas. Cuando d es un cuadrado perfecto, la ecuación 1.13 tiene sólo la solución trivial $(1, 0)$, por lo tanto siempre supondremos que d no es un cuadrado perfecto ($d > 0$). Dado que $x^2 - dy^2$ factoriza en los números reales como $\left(x - \sqrt{d}y\right)\left(x + \sqrt{d}y\right)$, es natural considerar esta ecuación en el dominio entero $\mathbb{Z}\left[\sqrt{d}\right]$, esto es, en el anillo de todos los números de la forma $x+y\sqrt{d}$, con $x, y \in \mathbb{Z}$. La representación de un $\alpha \in \mathbb{Z}\left[\sqrt{d}\right]$ como $\alpha = a+b\sqrt{d}$ es única, debido a que $\sqrt{d}$ es irracional. Los números a y b se llaman *componentes* de α. Sea $\alpha = x+y\sqrt{d}$; el número $x-y\sqrt{d}$ se conoce como el *conjugado de* α, denotado por $\overline{\alpha}$. El número $N(\alpha) = \alpha\overline{\alpha} = x^2-dy^2$ se llama la *norma* de α. De acuerdo a esta definición se sigue que *las soluciones de la ecuación de Pell son exactamente las componentes de los* $\alpha \in \mathbb{Z}\left[\sqrt{d}\right]$ *con* $N(\alpha) = 1$. Para estos α se cumple que su inverso multiplicativo es precisamente su conjugado. Además, $\alpha = x + y\sqrt{d}$ y $\alpha \geq 1$ implican que $x \geq 1$ y $y \geq 0$. Para ver esto observemos que $0 < \alpha^{-1} \leq 1$, $\alpha + \overline{\alpha} = 2x$ y $\alpha - \overline{\alpha} = 2y\sqrt{d}$. De esto se sigue que $x, y \geq 0$. Finalmente $x = \sqrt{1 + dy^2} \geq 1$. Así, $\alpha \geq 1$ implica que sus componentes son enteros no negativos. Como $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$, concluimos inmediatamente que $N(\alpha\beta) = N(\alpha)N(\beta)$. Lo cual implica que *el producto de elementos de* $\mathbb{Z}\left[\sqrt{d}\right]$*, que representen soluciones a la ecuación de Pell, es nuevamente un número cuyas componentes representan una solución a la ecuación de Pell.* También tenemos que $N(\alpha) = N(\overline{\alpha})$.

Sean $\alpha = x_1 + y_1\sqrt{d}$ y $\beta = x_2 + y_2\sqrt{d}$ dos soluciones de la ecuación de Pell, con $\alpha, \beta \geq 1$. Entonces, las ecuaciones $x_1^2 = dy_1^2 + 1$ y $x_2^2 = dy_2^2 + 1$ implican que $x_1 < x_2 \Leftrightarrow y_1 < y_2$, y por lo tanto, $1 \leq \alpha < \beta \Leftrightarrow 1 \leq x_1 < x_2$ y $1 \leq y_1 < y_2$. De aquí que el conjunto de los números reales α para los cuales $N(\alpha) = 1$ y $\alpha > 1$ sea un conjunto bien ordenado. Si este conjunto es no vacío, es decir, si existen soluciones no triviales a la ecuación de Pell, entonces debe existir un real minimal α tal que $N(\alpha) = 1$ y $\alpha > 1$. Este número se llama *el generador y sus componentes se llaman, la solución fundamental.*

Veamos que las potencias de α generan todas las soluciones de la ecuación 1.13. Primero observemos que las potencias de α representan también soluciones de (1.13). Sea β una solución de (1.13); como $\alpha > 1$, existe un natural n tal que $\alpha^n \leq \beta < \alpha$. De aquí se sigue que $1 \leq \beta\alpha^{-n} < \alpha$ y

$$N\left(\beta\alpha^{-n}\right) = N(\beta)\,N\left(\alpha^{-1}\right)^n = N(\beta)\,N(\alpha)^n = 1.$$

De la minimalidad de α concluimos que $\beta\alpha^{-n} = 1$, es decir, $\beta = \alpha^n$. No es trivial probar que

si d no es un cuadrado perfecto existe una solución no trivial a la ecuación 1.13. Este es un resultado estandar en la teoría clasica de números que no demostraremos. Sin embargo, para los propósitos de este capítulo es suficiente demostrar la existencia de soluciones no triviales cuando d tiene la forma especial $d = a^2 - 1$, con $a \in \mathbb{N}$.

La ecuación de Pell especial

$$x^2 - \left(a^2 - 1\right) y^2 = 1, \tag{1.14}$$

tiene la solución fundamental $(x, y) = (a, 1)$, ya que cualquier solución no trivial de (1.14) tiene segunda componente mayor que uno. De este modo su generador es $a + \sqrt{a^2 - 1}$. De lo anterior concluimos que las potencias de este número generan todas las soluciones de (1.14),

$$X_a(n) + Y_a(n)\sqrt{a^2 - 1} = \left(a + \sqrt{a^2 - 1}\right)^n. \tag{1.15}$$

Además, deducimos que $X_a(n)$ y $Y_a(n)$ son, como funciones de n, estrictamente crecientes.

Tomando el conjugado a ambos lados de (1.15) vemos que las sucesiones $X_a(n)$ y $Y_a(n)$ también son definibles a partir del conjugado del generador, $a - \sqrt{a^2 - 1}$, esto es,

$$X_a(n) - Y_a(n)\sqrt{a^2 - 1} = \left(a - \sqrt{a^2 - 1}\right)^n. \tag{1.16}$$

Como habíamos mencionado antes, el conjugado del generador es igual a su inverso,

$$a - \sqrt{a^2 - 1} = \left(a + \sqrt{a^2 - 1}\right)^{-1}. \tag{1.17}$$

Este hecho implica que la mayoría de las identidades que se pueden demostrar para las secuencias de soluciones de ecuaciones de Pell, se pueden demostrar también para valores negativos del parámetro n. Por ejemplo, de las identidades

$$\begin{aligned} \left(a + \sqrt{d}\right)^{n+m} &= \left(a + \sqrt{d}\right)^n \left(a + \sqrt{d}\right)^m, \\ \left(a + \sqrt{d}\right)^{n-m} &= \left(a + \sqrt{d}\right)^n \left(a + \sqrt{d}\right)^{-m} \end{aligned}$$

y usando las ecuaciones 1.15,1.16 y 1.17 obtenemos la identidad

$$X_a(n \pm m) + Y_a(n \pm m)\sqrt{d} = \left(X_a(n) + Y_a(n)\sqrt{d}\right)\left(X_a(m) \pm Y_a(m)\sqrt{d}\right). \tag{1.18}$$

Igualando las partes racionales e irracionales de la ecuación 1.18, obtenemos las *ecuaciones aditivas* (Lucas).

$$X_a(n \pm m) = X_a(n) X_a(m) \pm d Y_a(n) Y_a(m), \tag{1.19}$$

$$Y_a(n \pm m) = Y_a(n) Y_a(m) \pm X_a(n) Y_a(m). \tag{1.20}$$

En las ecuaciones 1.18, 1.19 y 1.20 los signos se corresponden.

Estas ecuaciones se cumplen para $a \geq 2$. Si definimos $X_1(n) = 1$ y $Y_1(n) = n$, entonces la identidad (1.20) también se cumplirá para $a = 1$. Haciendo $m = 1$ en (1.19) y (1.20) obtenemos un caso especial bastante útil:

$$X_n(n+1) = aX_a(n) + dY_a(n),\ Y_a(n+1) = aY_a(n) + X_a(n), \tag{1.21}$$

$$X_a(n-1) = aX_a(n) - dY_a(n),\ Y_a(n-1) = aY_a(n) - X_a(n). \tag{1.22}$$

Sumando las parejas de ecuaciones 1.21 y 1.22 podemos representar las sucesiones $X_a(n)$ y $Y_a(n)$ como secuencias de Lucas, es decir, secuencias modeladas por ecuaciones de recurrencia lineales de segundo orden:

$$X_a(0) = 1,\ X_a(1) = a,\ X_a(n+1) = 2aX_a(n) - X_a(n-1), \tag{1.23}$$

$$Y_a(0) = 1,\ Y_a(1) = a,\ Y_a(n+1) = 2aY_a(n) - Y_a(n-1). \tag{1.24}$$

De las ecuaciones aditivas (1.19) y (1.20), junto con la ecuación 1.14, deducimos las *fórmulas de ángulo doble* (Lucas)

$$X_a(2n) = 2X_2(n)^2 - 1, \tag{1.25}$$

$$Y_a(2n) = 2X_a(n) Y_a(n). \tag{1.26}$$

En virtud de (1.24), si fijamos a n, la función $Y_a(n)$ es un polinomio en a de grado $n-1$. De este hecho obtenemos la llamada regla de congruencia,

$$Y_a(n) \equiv Y_b(n) \bmod(a-b). \tag{1.27}$$

La regla de congruencia se cumple para $a, b \geq 1$. Haciendo $b = 1$ en (1.27) y usando el hecho de que $Y_1(n) = n$ obtenemos la regla de recurrencia especial de Julia Robinson:

$$Y_a(n) \equiv n \bmod(a-1). \tag{1.28}$$

Las ecuaciones de Lucas 1.23 y 1.24, nos permiten estimar cotas para el tamaño de las secuencias X_a y Y_a. Por ejemplo, es sencillo demostrar las siguientes cotas para la sucesión

$Y_a(n)$:

$$(2a-1)^n \leq Y_a(n+1) < (2a)^n . \tag{1.29}$$

Esta desigualdad, la cual se cumple para $a \geq 1$ y $n > 1$, muestra que la secuencia $Y_a(n)$ crece exponencialmente en n. Estas secuencias, $Y_a(n)$ y $X_a(n)$, pueden relacionarse de modo más directo con la función exponencial. La siguiente congruencia fue demostrada por Julia Robinson [21]

$$X_a(n) - (a-k) Y_a(n) \equiv k^2 \bmod(2ak - k^2 - 1). \tag{1.30}$$

Prueba. Mostraremos que la congruencia es válida para cada $k, n \geq 0$. Es fácil verificarla para $n = 0, 1$. Así, usando inducción y las fórmulas 1.23 y 1.24, obtenemos

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

■

Ahora probraremos una propiedad de divisibilidad que usaremos en la demostración de nuestro primer lema fundamental.

$$n|m \Leftrightarrow Y_a(n) \,|Y_a(m) . \tag{1.31}$$

Prueba. De la ecuación aditiva 1.20 tenemos que (omitiendo el subíndice a)

$$Y(k \pm n) = Y(k) X(n) \pm X(k) Y(n) \pm Y(k) X(n) (\bmod Y(n)) .$$

Pero $Y(n) \perp X(n)$, debido a la ecuación 1.14. Así,

$$Y(n) \,|Y(n \pm k) \Leftrightarrow Y(n) \,|Y(k) .$$

Sea $m = ni + r$, con $0 \leq r < n$. Entonces, $0 \leq Y(r) < Y(n)$. Luego,

$$Y(n) \,|Y(m) \Leftrightarrow Y(n) \,|Y(ni + r) \Leftrightarrow Y(n) \,|Y(r) .$$

De este modo, $Y(n) \,|Y(m)$ si y sólo si $r = 0$, es decir, si $n|m$. ■

Lema 1.3.1 ***(Primer Lema Fundamental)*** *Para $a \geq 0$ tenemos que*

$$Y_a^2(n) \,|Y_a(m) \Leftrightarrow nY_a(n) \,|m. \tag{1.32}$$

Prueba. Usando la ecuación 1.15 vemos que para cada j,

$$Y_a(nj) = \sum_{i=1,impar}^{j} \left(\begin{array}{c} j \\ i \end{array} \right) X_a(n)^{j-1} Y_a(n)^i \left(\sqrt{d}\right)^{i-1}.$$

Por lo tanto,

$$Y_a(nj) \equiv jX_a(n)^{j-1} Y_a(n) \left(\mathrm{mod}\, Y_a(n)^3\right). \tag{1.33}$$

Supongamos que $Y(n)^2 | Y(m)$. Luego, por (1.31) $m = nj$, para algún j. Fijemos este j en (1.33). Como $X(n) \perp Y(n)$, (1.33) implica que $Y(n)^2 | jY(n)$, es decir, $Y(n) | j$, con lo cual $nY(n) | m$. Recíprocamente, supongamos que $nY(n) | m$. Sea $j = Y(n)$. Por (1.33) se tiene que $Y(n)^2 | Y(nY(n))$. Pero, por (1.32) $Y(nY(n)) | Y(m)$. Así, $Y(n)^2 | Y(m)$. ■

Lema 1.3.2 *Para $a \geq 2$ y $n \geq 1$, tenemos que $Y_a(n-1) + Y_a(n) < X_a(n)$.*

Prueba. Reemplazamos n por $n-1$ en (1.21) para obtener $aY(n-1) + X(n-1) = Y(n)$. Para $n \geq 2$, tenemos que

$$2Y(n-1) \leq aY(n-1) < aY(n-1) + X(n-1) = Y(n),$$

de donde $Y(n-1) < Y(n-1) - Y$. Sumamos $Y(n)$ a ambos lados para obtener

$$Y(n-1) + Y(n) < 2Y(n) + Y(n-1) \leq aY(n) - Y(n-1) = X(n),$$

por (1.24). ■

Lema 1.3.3 $Y_a(4nj \pm m) \equiv \pm Y_a(m)$ *y* $Y_a(4nj + 2n \pm m) \equiv \mp Y_a(m) (\mathrm{mod}\, X_a(n))$.

Prueba. De (1.26) y (1.25) tenemos que

$$Y(2n) \equiv 0 (\mathrm{mod}\, X(n)) \text{ y } X(2n) \equiv -1 (\mathrm{mod}\, X(n)),$$

respectivamente. Así, por (1.20) obtenemos

$$Y_a(2n \pm m) \equiv Y(2n) X(m) \pm X(2n) Y(m) \equiv \mp Y(m) (\mathrm{mod}\, X(n)).$$

Ahora

$$Y(4n \pm m) \equiv Y(2n + 2n \pm m) \equiv -Y(2n \pm m) \equiv \pm Y(m) (\mathrm{mod}\, X(n)),$$

o sea, $Y_a(4n \pm m) \equiv \pm Y_a(m) (\mathrm{mod}\, X(n))$. Aquí los signos se corresponden. ■

En el siguiente lema fundamental los signos *no se corresponden.*

Lema 1.3.4 *(**Segundo Lema Fundamental**)*$Y_a(k) \equiv \pm Y_a(m) \pmod{X(n)}$ *es equivalente a que* $k \equiv \pm m \pmod{2n}$.

Prueba. Supondremos, como es usual, que $a \geq 2$ y $n \geq 1$. Para la demostración de la implicación $\Leftarrow$, supongamos que $k = 2nj \pm m$. Cuando $j = 2i$, tenemos que

$$Y(k) \equiv Y(4ni \pm m) \equiv \pm Y(m) \pmod{X(n)}.$$

En el caso de que $j = 2i + 1$, obtenemos

$$Y(k) = Y(4ni + 2n \pm m) \equiv Y(m) \pmod{X(n)}.$$

Así, $Y(k) \equiv Y \pmod{X(n)}$.

Para la otra dirección, supongamos que $Y(k) \equiv \pm Y(m) \pmod{X(n)}$. Escogamos k y m tales que

$$0 \leq k', m' \leq n, k \equiv \pm k' \pmod{2n} \text{ y } m \equiv \pm m' \pmod{2n}.$$

Luego, de la hipótesis y "$\Leftarrow$" tenemos que $Y(k') \equiv \pm Y(m) \pmod{X(n)}$. Luego, $X(n) | Y(k') \pm Y(m)$, así $k' = m$, porque si fueran distintos tendríamos que

$$0 < |Y(k') \pm Y(m')| \leq Y(k') + Y(m') \leq Y(n-1) + Y(n) < X(n),$$

por el lema 1.3.2. De $k' = m'$ deducimos que $k \equiv \pm m \pmod{2n}$. ■

Lema 1.3.5 *Para* $A > 1$ *se cumple* $C = Y_A(B)$ *si y sólo si existen números naturales* D, E, F, G, H, I, i *tales que*

$$D^2 - (A^2 - 1) C^2 = 1, \tag{1.34}$$

$$F^2 - (A^2 - 1) E^2 = 1, \tag{1.35}$$

$$I^2 - (G^2 - 1) H^2 = 1, \tag{1.36}$$

$$E = (i + 1) 2C^2, \tag{1.37}$$

$$G \equiv A \pmod{F}, \tag{1.38}$$

$$G \equiv 1 \pmod{2C}, \tag{1.39}$$

$$H \equiv C \pmod{F}, \tag{1.40}$$

$$H \equiv B \pmod{2C}, \tag{1.41}$$

$$B \leq C. \tag{1.42}$$

Prueba. Suficiencia. Supongamos que existen D, E, F, G, H, I, i que satisfacen las ecuaciones (1.34) a (1.42). Las ecuaciones (1.34) a (1.36), ecuaciones de Pell, implican la existencia de números p, q y r tales que

$$D = X_A(p), C = Y_A(p), F = X_A(q), E = Y_A(q), I = X_G(r)$$

y $H = Y_G(r)$. También $0 \leq p \leq C$ y $0 \leq B \leq C$. De este modo, la idea es probar que $B = p$, mostrando $B \equiv r \equiv \pm p \pmod{2C}$. Podemos suponer que $C > 0$. Usando el primer lema fundamental y la ecuación 1.37, deducimos la siguiente cadena de implicaciones

$$C^2 | E \Rightarrow Y_A^2(p) | Y_A^2(q) \Rightarrow Y_A(p) | q \Rightarrow C | q.$$

Usando (1.39), (1.41) y la regla de congruencia se tiene que

$$B \equiv H = Y_G(r) = r \pmod{2C} \Rightarrow B \equiv r \pmod{2C}. \tag{1.43}$$

En virtud del segundo lema fundamental, la regla de congruencia, 1.38 y 1.40

$$Y_A(r) \equiv Y_G(r) \equiv H \equiv C = Y_A(p) \pmod{X_A(q)},$$

luego $r \equiv \pm p \pmod{2q}$. Pero sabemos que $C|q$. Así, $r \equiv \pm p \pmod{2C}$. Este hecho junto con (1.43) implican que $B \equiv \pm p \pmod{2C}$. Recíprocamente, supongamos que $C = Y_A(B)$. Sea $A = X_A(B)$. Entonces, (1.34) y (1.42) se cumplen. Definamos $q = BY_A(B), F = X_A(2q)$ y $E = Y_A(2q)$. Luego (1.35) se cumple. Sea $m = BY_A(B)$ en el primer lema fundamental. Asi, el primer lema fundamental dice que $Y_A(B)^2 | Y_A(BY_A(B))$.

Por lo tanto, $C^2 | Y_A(q)$. La fórmula de ángulo doble (1.26) afirma que $2X_A(q) Y_A(q) | Y_A(2q)$. Luego $2C^2 | E$, de este modo se cumple 1.37. Sea $G = A + F^2(F^2 - A)$, entonces (1.38) es cierta. (1.35) y (1.37) implican que $F^2 \equiv 1 \pmod{2C}$. Así, la definición de G hace que (1.39) sea verdad. Definamos $I = X_G(B)$ y $H = Y_G(B)$. De este modo, se cumple (1.36). De (1.28) $H = Y_G(B) \equiv B \pmod{G-1}$, así por (1.39), $H \equiv B \pmod{2C}$ y en consecuencia 1.41 es verdad. Además, $H = Y_G(B) = Y_A(B) \equiv C \pmod{G-A}$, en virtud de la regla de congruencia. Este hecho sumado a (1.38) implica que $H \equiv C \pmod{F}$, es decir, se cumple (1.41). De lo anterior se concluye la validez del lema. ■

1.4 El Coeficiente Binomial y la Relación Exponencial

Por el lema 1.3.5, la relación entre variables, $y = Y_a(n)$ es diofantina. Luego, podemos usarla para mostrar que otras relaciones son diofantinas. Además, del lema 1.3.5 y la ecuación 1.14 se sigue inmediatamente que la relación $x = X_a(n)$ es diofantina. Usaremos estas dos relaciones

para demostrar que la relación exponencial, $m = k^n$ es diofantina.

Lema 1.4.1 *Supongamos que $n \geq 1, k \geq 2$. Entonces para todo $a \geq Y_k(n+1)$,*

$$k^n = res\left(X_a(n) - (a-k)\,Y_a(n), 2ak - k^2 - 1\right).$$

Prueba. De 1.29, tenemos que $k \leq k^n < (2k-1)^n \leq Y_k(n+1) \leq a$ y por lo tanto $k+1 \leq a$, de lo cual se sigue que

$$a < ak < ak + k - 1 = ak + (k+1)\,k - k^2 \leq ak + ak - k^2 - 1 = 2ak - k^2 - 1.$$

Así, $k^2 < 2ak - k^2 - 1$, luego k^n es menor que el módulo. Ahora, en virtud de la congruencia 1.30,

$$k^n \equiv X_a(n) - (a-k)\,Y_a(n) \left(\mathrm{mod}\, 2ak - k^2 - 1\right).$$

Como k^n es menor que el módulo se sigue que tiene que ser igual al residuo buscado. ■

Teorema 1.4.2 *La relación exponencial, $m = k^n$, con $n \geq 1, k \geq 2$ y $m \geq 2$ es diofantina.*

Prueba. En virtud del lema 1.4.1, $m = k^n$ si y sólo si existe un a tal que

$$m \equiv X_a(n) - (a-k)\,Y_a(n) \left(\mathrm{mod}\, 2ak - k^2 - 1\right), m > a, a \geq Y_k(n+1).$$

Luego, del lema 1.3.5, y las expresiones 1.11, 1.12 se sigue que la relación $m = k^n$ es diofantina. ■

A continuación mostraremos que la relación en tres variables, $m = \begin{pmatrix} n \\ k \end{pmatrix}$, es diofantina. Julia Robinson fue la primera persona en probar que esta relación era exponencial diofantina. La idea básica de la prueba es el hecho de que los coeficientes binomiales son los dígitos en la expansión en base u de $(1+u)^n$, para u suficientemente grande. El símbolo $\lfloor x \rfloor$, para x un número real positivo, denota el mayor entero menor o igual a x.

Lema 1.4.3 *Para $0 \leq 1 \leq n$ y $u > 2^n$,*

$$\begin{pmatrix} n \\ k \end{pmatrix} = res\left(\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor, u\right). \tag{1.44}$$

Prueba. Al expandir $(u+1)^n$ y divir por u^k obtenemos

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

de esto y la desigualdad $u^{i-k} \leq 1/u$, la cual se cumple para $i \leq k-1$, tenemos

$$\sum_{i=0}^{k-1} \left(\begin{array}{c} n \\ i \end{array} \right) u^{i-k} \leq \frac{1}{u} \sum_{i=0}^{k-1} \left(\begin{array}{c} n \\ i \end{array} \right) \leq \frac{1}{u} \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) = \frac{2^n}{u} < 1.$$

Por lo tanto,

$$\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \equiv \left(\begin{array}{c} n \\ k \end{array} \right) (\mathrm{mod}\, u)\,.$$

Así, en virtud de $\left(\begin{array}{c} n \\ k \end{array} \right) \leq 2^n < u$, deducimos el lema. ■

Para algunos resultados posteriores, necesitaremos una definición un poco más amplia de $\left(\begin{array}{c} a \\ b \end{array} \right)$. Si $0 \leq a < b$, entonces definimos $\left(\begin{array}{c} a \\ b \end{array} \right)$ como cero. Nótese que la ecuación 1.44 no es válida en el sentido extendido, ya que si fijamos $n > 0$ y $k > 2^n$, entonces, para $k = n+1$, se tendría que

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

lo cual implicaría que

$$res\left(\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor, u \right) = 1 \neq \left(\begin{array}{c} n \\ n+1 \end{array} \right).$$

Teorema 1.4.4 *La relación binomial* $m = \left(\begin{array}{c} n \\ k \end{array} \right)$, *en el sentido extendido, es diofantina.*

Prueba. En virtud del Lema 1.4.3, tenemos que $m = \left(\begin{array}{c} n \\ k \end{array} \right)$, si y sólo si, existe u, x y y tales que

$$[n < k \wedge m = 0] \vee \left[n \geq k \wedge (u+1)^n = yu^{k+1} + mu^k + x \wedge u > 2^n \wedge u^k > x \wedge u > m \right].$$

Luego, en virtud del teorema 1.4.2, la relación binomial es diofantina. ■

Ahora definiremos una relación binaria $\preccurlyeq$, que será fundamental en proceso de aritmetización de máquinas registradoras, lo cual explicaremos más adelante.

Definición 1.4.1 *Sean r y s números natruales escritos en binario. Entonces, $r \preccurlyeq s$ significa que cada dígito en binario de r es menor o igual que el correspondiente dígito en binario de s.*

Claramente si $a \preccurlyeq b$, entonces $a \leq b$. A continuación veremos que la relación $a \preccurlyeq b$ es diofantina, pero primero probaremos un teorema de Lucas sobre los coeficientes binomiales módulo un primo.

Teorema 1.4.5 ***(Lucas, 1878)*** *Sean p un número primo y r_i, s_i los dígitos en base p de r y s, respectivamente. Entonces*

$$\left(\begin{array}{c} s \\ r \end{array} \right) \equiv \left(\begin{array}{c} s_n \\ r_n \end{array} \right) \ldots \left(\begin{array}{c} s_1 \\ r_1 \end{array} \right) \left(\begin{array}{c} s_0 \\ r_0 \end{array} \right) (\mathrm{mod}\, p)\,.$$

Prueba. Por inducción, es suficiente demostrar que dados b y d tales que $0 \leq b, d < p$, se cumple

$$\left(\begin{array}{c} ap+b \\ cp+d \end{array} \right) \equiv \left(\begin{array}{c} a \\ c \end{array} \right) \left(\begin{array}{c} b \\ d \end{array} \right) (\mathrm{mod}\, p)\,.$$

Primero supongamos que $a \geq c$ y $b \geq d$. Consideremos el coeficiente del término x^{cp+d} en el polinomio $(1+x)^{ap+b}$, visto como polinomio en el anillo $\mathbb{Z}_p[x]$. De la igualdad $(x+y)^p = x^p + y^p$ obtenemos

$$\begin{aligned} \sum_{n=0}^{ap+b} \left(\begin{array}{c} ap+b \\ n \end{array} \right) x^n &= (1+x)^{ap+b} = (1+x)^{ap} (1+x)^b = (1+x^p)^a (1+x)^b \\ &= \left(\sum_{j=0}^{a} \left(\begin{array}{c} a \\ j \end{array} \right) x^{jp} \right) \left(\sum_{i=0}^{b} \left(\begin{array}{c} b \\ i \end{array} \right) x^i \right) = \sum_{j=0}^{a} \sum_{i=0}^{b} \left(\begin{array}{c} a \\ j \end{array} \right) \left(\begin{array}{c} b \\ i \end{array} \right) x^{jp+i}. \end{aligned}$$

Ahora, la ecuación $jp+i = cp+d$ sólo se puede cumplir para $j = c$ y $d = i$, ya que $0 \leq i \leq b < p$ y $0 \leq d < p$. Por lo tanto, el coeficiente de x^{cp+d} en $(1+x)^{ap+b}$ debe ser $\left(\begin{array}{c} a \\ c \end{array} \right) \left(\begin{array}{c} b \\ d \end{array} \right)$. Así,

$$\left(\begin{array}{c} ap+b \\ cp+d \end{array} \right) = \left(\begin{array}{c} a \\ c \end{array} \right) \left(\begin{array}{c} b \\ d \end{array} \right)$$

es válida en $\mathbb{Z}_p$.

Supongamos que $0 \leq a < c$. Luego

$$(ap+b) - (cp+d) = p\,(a-c) + (b-d) \leq -p + (b-d) < 0.$$

Así, por definición

$$\left(\begin{array}{c} ap+b \\ cp+d \end{array} \right) = 0 = \left(\begin{array}{c} a \\ c \end{array} \right),$$

y por tanto, la congruencia se cumple de manera trivial. Finalmente, supongamos que $0 \leq c \leq a$ y $b < d$. Por un teorema de Kummer la potencia más alta de p que divide a $\binom{m}{n}$ $(m \geq n)$ es

$$\sum_{i=1}^{\infty} \left(\left\lfloor \frac{m}{p^i} \right\rfloor - \left\lfloor \frac{m-n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^i} \right\rfloor \right). \tag{1.45}$$

Si $a = c$, suponiendo que $b < d$, la congruencia se cumple trivialmente, ya que ambos lados son cero. Así podemos suponer que $a > c \geq 0$, y por lo anterior, tenemos que $ap + b > cp + d$, y podemos usar (1.45). Primero, notemos que cada término de (1.45) es un entero no negativo debido a que $\lfloor m+n \rfloor - \lfloor m \rfloor - \lfloor n \rfloor \geq 0$, para cada $m, n \in \mathbb{N}$. Ahora, en nuestro caso

$$\begin{aligned} \sum_{i=1}^{\infty} \left(\left\lfloor \frac{ap+b}{p^i} \right\rfloor - \left\lfloor \frac{ap+b-(cp+d)}{p^i} \right\rfloor - \left\lfloor \frac{cp+d}{p^i} \right\rfloor \right) &\geq \left\lfloor \frac{ap+b}{p} \right\rfloor - \left\lfloor \frac{ap+b-(cp+d)}{p} \right\rfloor - \left\lfloor \frac{cp+d}{p} \right\rfloor \\ &= \left\lfloor a + \frac{b}{p} \right\rfloor - \left\lfloor a - c + \frac{b-d}{p} \right\rfloor - \left\lfloor c + \frac{d}{p} \right\rfloor \\ &= a - (a - c - 1) - c = 1, \end{aligned}$$

ya que $-1 < \dfrac{b-c}{p} < 0$. Esto significa que $p | \binom{ap+b}{cp+d}$, luego la congruencia se cumple ya que $\binom{b}{d} = 0$. De este modo se concluye la demostración. ■

Teorema 1.4.6 *Para r, s números naturales se cumple la siguiente equivalencia:*

$$r \preccurlyeq s \Leftrightarrow \binom{s}{r} \equiv 1 \pmod 2. \tag{1.46}$$

Y, de este modo, la relación $\preccurlyeq$ es diofantina.

Prueba. Haciendo $p = 2$ en el teorema 1.4.5, tenemos que 1.46 se sigue de las relaciones triviales

$$\binom{1}{0} = 0, \binom{1}{1} = 1, \binom{0}{0} = 1, \binom{0}{1} = 0.$$

■

1.5 Aritmetización de las máquinas registradoras

En este punto, tenemos suficientes relaciones diofantinas para probar que cada conjunto listable es diofantino. Existen muchas equivalencias de la definión de conjunto listable y función recursiva. La que usaremos aquí es la siguiente: *una función recursiva es una función que se puede*

computar con una máquina registradora. Un conjunto A es listable (r.e.) si $A = \emptyset$ o A es el rango de una función recursiva.

Una *máquina registradora* consiste en un programa finito y un número finito de registros completamente independientes $R1, R2, \ldots, Rr$. Los registros pueden contener números naturales arbitariamente grandes. Un subconjunto de registros, digamos $R1, R2, \ldots, Rk$ $(k < r)$ es designado como registros de entrada y un subconjunto, digamos $R1, R2, \ldots, Rm\,(m < r)$ es designado como registros de salida. Esto se hace para computar funciones de k variables cuyos valores son m-tuplas. Normalmente, $k = m = 1$, ya que $R1$ es considerado el registro de entrada-salida. Una máquina registradora es realmente un programa, *una lista de comandos escritos en líneas separadas,* etiquetadas como $L1, L2, \ldots, Ll$. Los comandos de la máquina, normalmente son ejecutados secuencialmente; sin embargo, la máquina registradora puede ejecutar comandos que le ordenen transferir el control a una línea distinta de la línea siguiente. Para efectos de computar todas las funciones recursivas, es suficiente suponer que las máquinas registradoras pueden sumar o restar 1 de un registro y cambiar de línea dependiendo del valor de nulidad de un registro, es decir, dependiendo de si un registro tiene un valor nulo o no lo tiene, sin importar el valor específico del mismo.

Un comando de resta puede causar problema si el valor que hay en el registro es cero en el momento de ejecutarlo. Por esta razón Minsky[14] permite ejecutar un comando de resta sólo después de un "test" de nulidad del correspondiente registro. Por esta razón, dicho comando requiere dos líneas

$$Li \qquad IF\ Rj = 0, GOTO\ Lk, \tag{1.47}$$

$$Li + 1 \qquad ELSE\ Rj \leftarrow Rj - 1, \tag{1.48}$$

para ser ejecutado. Es suficiente suponer que el programa está escrito de tal modo que la resta de un registro nulo nunca ocurra. Supondremos que una máquina registradora puede ejecutar los siguientes comandos:

Comando	Interpretación
$GOTO\ Lk$	Transferencia a la línea Lk
$IF\ Rj > 0\ GOTO\ Lk$	Condicional de transferencia a la línea Lk
$Rj \leftarrow Rj + 1$	Sumar al registro Rj una unidad
$Rj \leftarrow Rj - 1$	Restar al registro Rj una unidad

Para ahorrar un poco de espacio permitiremos que un comando del tipo $Rj \leftarrow Rj \pm 1$ se pueda, según el caso, escribir en una misma línea. Con el propósito de familiarizarnos un poco con este concepto daremos a continuación el ejemplo de una máquina registradora que computa el n-ésimo número de Fibonacci, F_n.

L1 IF $R1 = 0, GOTO$ L20

L2 $R2 \leftarrow R2 + 1, R3 \leftarrow R3 + 1$

L3 $R1 \leftarrow R1 - 1$

L4 IF $R1 = 0, GOTO$ L16

L5 $R1 \leftarrow R1 - 1$

L6 $R4 \leftarrow R4 + 1, R5 \leftarrow R5 + 1$

L7 $R3 \leftarrow R3 - 1$

L8 IF $R3 > 0, GOTO$ L6

L9 $R4 \leftarrow R4 + 1, R2 \leftarrow R2 - 1$

L10 IF $R2 > 0, GOTO$ L9

L11 $R3 \leftarrow R3 + 1, R4 \leftarrow R4 - 1$

L12 IF $R4 > 0, GOTO$ L11

L13 $R2 \leftarrow R2 + 1, R5 \leftarrow R5 - 1$

L14 IF $R5 > 0, GOTO$ L13

L15 IF $R1 > 0$, GOTO L5

L16 $R3 \leftarrow R3 - 1$

L17 IF $R3 > 0$, GOTO L16

L18 $R2 \leftarrow R2 - 1, R1 \leftarrow R1 + 1$

L19 IF $R2 > 0$, GOTO L18

L20 stop

Esta máquina M computa la función $f(x) = F_x$, donde $F_0 = 0, F_1 = 1$ y $F_x = F_{x-1} + F_{x-2}$. Si M es iniciada en la línea L1, con x en el registro $R1$ y cero en los demás registros, entonces M eventualmente se detendrá con F_x en el registro $R1$ y cero en los demás registros. Podemos entender esto como una definición general de computabilidad.

Para aritmetizar el trabajo de una máquina registradora, usaremos los dígitos de números esritos en base Q, donde Q es un potencia de 2. Consideremos la máquina M del ejemplo anterior o más generalmente cualquier máquina registradora con r registros y l líneas en su progama. Supongamos que M computa la función total $y = f(x)$, es decir, una función f con dominio el conjunto de los números naturales. Durante el cómputo, el contendio de los registros, en el tiempo t, nunca podrá exceder el valor de $x + t$. Así, usaremos el hecho de que después de s pasos de cómputo, el contenido de cada registro Ri es menor o igual a $x + s$.

Supongamos que después de s pasos, el valor $y = f(x)$ es obtenido por M. Denotemos por $r_{j,t}$, el contenido del registro Rj en el tiempo t durante el curso de la computación. Si Q es suficientemente grande, tendríamos que $r_{j,t} < Q$, para cada j y durante cada tiempo t en el cómputo. De este modo, los números $r_{j,t}$ pueden ser considerados como los dígitos de un número escrito en base Q. Pero, por una razón que se entenderá más adelante, necesitaremos más espacio, o sea, requeriremos que $2r_{j,t} < Q$. Por lo tanto, haremos que Q satisfaga lo

siguiente:

$$x + s < Q/2, \tag{1.49}$$

$$l + 1 < Q, \tag{1.50}$$

$$Q = 2^w, \text{ para algún } w \in \mathbb{N}. \tag{1.51}$$

Aquí, l denota el número de líneas del programa. Por ejemplo, el número $Q = 2^{x+s+l+1}$ es suficientemente grande para nuestros fines. Para describir la línea que está ejecutando la máquina M en el instante o tiempo t, definimos $l_{j,t}$ como 1 ó 0, dependiendo de que la máquina M, esté o no, en la línea Lj en el instante t. Así, cuando la máquina M comience a computar se iran generando números Rj y Li de la siguiente manera:

$$Rj = \sum_{t=0}^{s} r_{j,t} Q^t \qquad (0 \leq r_{j,t} < Q/2)\,, \tag{1.52}$$

$$Li = \sum_{t=0}^{s} l_{i,t} Q^t \qquad (0 \leq l_{i,t} < 1)\,, \tag{1.53}$$

donde $1 \leq j \leq r$, con r igual al número de registros; $1 \leq i \leq l$.

Nos será de gran utilidad utilizar el número I, el cual escrito en base Q tenga todos sus dígitos iguales a 1. La serie geométrica nos permitirá obtener este valor de manera diofantina, es decir,

$$1 + (Q-1)\, I = Q^{s+1}, \tag{1.54}$$

si y sólo si, $I = \sum_{t=0}^{s} Q^t$.

Para poder utilizar la aritmetización, consideremos la máquina registradora de nuestro ejemplo anterior. Esta máquina tiene $r = 5$ registros y $l = 19$ líneas de programa. Si la máquina comienza a computar con $x = 2$ en el registro $R1$ y cero en los demás, entonces ésta se detendrá a los $s = 23$ pasos con 1 en el registro $R1$ y cero en los demás ($F_2 = 1$). Durante el cómputo de F_2 la máquina generará los siguientes números R_1, R_2, R_3, R_4, R_5, representando contenidos de los registros, durantes los diferentes pasos o instantes, en el sentido de (1.52). Estos números escritos en base Q tendrán la siguiente forma:

$$\begin{aligned}
R_1 &= 110000000000000000011222,\\
R_2 &= 001111111000000111111100,\\
R_3 &= 000011222221100001111100,\\
R_4 &= 000000000001122111000000,\\
R_5 &= 000000000111111111000000.
\end{aligned}$$

Similarmente, se generaran números representando las líneas que ejecutó el programa en cada

paso. Estos números en base Q serán:

$$
\begin{aligned}
L_1 &= 000000000000000000000001,\\
L_2 &= 000000000000000000000010,\\
L_3 &= 000000000000000000000100,\\
L_4 &= 000000000000000000001000,\\
L_5 &= 000000000000000000010000,\\
L_6 &= 000000000000000000100000,\\
L_7 &= 000000000000000001000000,\\
L_8 &= 000000000000000010000000,\\
L_9 &= 000000000000000100000000,\\
L_{10} &= 000000000000001000000000,\\
L_{11} &= 000000000001010000000000,\\
L_{12} &= 000000000010100000000000,\\
L_{13} &= 000000001000000000000000,\\
L_{14} &= 000000010000000000000000,\\
L_{15} &= 000000100000000000000000,\\
L_{16} &= 000010100000000000000000,\\
L_{17} &= 000101000000000000000000,\\
L_{18} &= 001000000000000000000000,\\
L_{19} &= 010000000000000000000000,\\
L_{20} &= 100000000000000000000000.
\end{aligned}
$$

Notemos que los números $L_1, L_2, \ldots, L_{20}, R_1, R_2, \ldots, R_5$ contienen toda la historia del cómputo realizado por la máquina registradora para $x = 2$.

Ahora, mostraremos como escribir condiciones diofantinas en variables arbitrarias $L_1, \ldots, L_{20}$, $R_1, \ldots, R_5, s, Q, x, y$ suficientes como para forzarlas a ser estos valores particulares. Es decir, daremos condiciones diofantinas en estas variables, las cuales se satisfacen, si y sólo si, para la entrada x, la máquina M produce el valor $y = f(x)$.

En general, las variables desconocidas en estas relaciones diofantinas serán entre otras, $s, Q, I, R_1, R_2, \ldots, R_r, L_1, L_2, \ldots, L_{l+1}$. Los números r y l serán constantes, por ejemplo, $r = 5$ y $l = 19$, para la máquina que describimos anteriormente. Después de escribir estas condiciones, los métodos de las secciones anteriores nos permitirán traducirlas en ecuaciones diofantinas, en

estas y más variables desconocidas. Nuestras primeras 4 condiciones serán (1.49), (1.50), (1.51) y (1.55). Ahora, para hacer que un número natural arbitrario R_j cumpla la condición , usaremos la relación $\preccurlyeq$ y el hecho de que $a \preccurlyeq b$ implica que cada dígito de a, en base Q, es menor o igual que el correspondiente dígito de b.

$$R_j \preccurlyeq \left(\frac{Q}{2} - 1\right) I \qquad (j = 1, 2, \ldots, r)\,. \tag{1.55}$$

Como Q es una potencia de 2, esta condición es otra manera de presentar la condición (1.52). También, es necesario hacer que en cada columna de la matriz que forman los dígitos de los valores $L_1, L_2, \ldots, L_{l+1}$; haya exactamente un 1 y el resto lleno de ceros. Dado que $1 < Q$, por (1.50), podemos usar las siguientes dos condiciones para este fin:

$$I = \sum_{i=1}^{l+1} L_i, \tag{1.56}$$

$$L_i \preccurlyeq I \qquad (i = 1, 2, \ldots, l + 1)\,. \tag{1.57}$$

Para inicializar la máquina en la línea L_1, pondremos la siguiente condición de inicio:

$$Q \preccurlyeq L_1. \tag{1.58}$$

Con relación a los comandos GOTO podemos suponer que hay sólo una instrucción de parada, localizada al final de programa. La condición de parada de la máquina después de s pasos será:

$$L_{l+1} = Q^s. \tag{1.59}$$

Para simular comandos de la forma Li GOTO Lk, incluimos la condición

$$QL_i \preccurlyeq L_k. \tag{1.60}$$

Esta instrucción obliga a que el dígito $t+1$-ésimo de L_k sea 1, siempre que el dígito t-ésimo de L_i sea 1. Para comandos de la forma Li IF $Rj > 0, GOTO\ L_k$ una idea un poco más fina que la anterior funciona. Asumamos que $k \neq i + 1$, para que el comando no sea trivial. Usaremos, en este caso el siguiente par de instrucciones:

$$QL_i \preccurlyeq L_k + L_{i+1} \text{ y } QL_i \preccurlyeq L_k + QI - 2Rj. \tag{1.61}$$

La primera condición fuerza la transferencia a la línea L_k o L_{i+1} y la segunda decide a cual de las dos se transferirá. Para entender como funcionan estas condiciones, hagamos el siguiente

diagrama (fijando por un momento una máquina registradora $\overline{M}$)

	$\overline{Q}=2^6$	$\overline{Q}^6$		$\overline{Q}^5$		$\overline{Q}^4$		$\overline{Q}^3$		$\overline{Q}^2$		$\overline{Q}^1$		$\overline{Q}^0$
$\overline{I}=$	00000	0	00000	1	00000	1	00000	1	00000	1	00000	1	00000	1
$\overline{Q}.\overline{I}=$	00000	1	00000	1	00000	1	00000	1	00000	1	00000	1	00000	0
$2\overline{R_i}=$	00000	0	*****	0	*****	0	*****	0	*****	0	*****	0	*****	0

La idea es que cuando $r_{j,t}>0$ restar $2R_j$ de QI hace que se sustraiga un dígito de la posición Q^{t+1} de QI. Por ejemplo, supongamos que los únicos dígitos no nulos de $\overline{R_j}$, en base $\overline{Q}$, son $r_{j,3}, r_{j,4}, r_{j,5}$. Luego, $\overline{QI}-2\overline{R_j}$, escrito en base 2, tendrá la siguiente forma:

		$\overline{Q}^6$		$\overline{Q}^5$		$\overline{Q}^4$		$\overline{Q}^3$		$\overline{Q}^2$		$\overline{Q}^1$		$\overline{Q}^0$
$\overline{I}=$	00000	0	*****	0	*****	0	*****	1	00000	1	00000	1	00000	0

Además, supongamos que para cierta línea $\overline{L}i$, el valor de $\overline{L_i}$ está dado, escrito en base 2,

		$\overline{Q}^6$		$\overline{Q}^5$		$\overline{Q}^4$		$\overline{Q}^3$		$\overline{Q}^2$		$\overline{Q}^1$		$\overline{Q}^0$
por $\overline{L}_i=$	00000	0	00000	0	00000	0	00000	1	00000	0	00000	1	00000	0
$\overline{QL}_i=$	00000	0	00000	0	00000	1	00000	0	00000	1	00000	0	00000	0

Supongamos que $\overline{M}$ tiene una línea de la forma $\overline{L}i\ IF\ \overline{R}i>0\ GOTO\ \overline{L}k$, y además

$$\overline{QL}_i \preccurlyeq \overline{L}_k+\overline{L}_{i+1},$$

$$\overline{QL}_i \preccurlyeq \overline{L}_k+\overline{QI}-2\overline{R}_j. \tag{1.62}$$

En el ejemplo sabemos que $\overline{L}_{i,1}=1$ y $\overline{r}_{j,1}=0$, luego, si $\overline{L}_{k,2}=1$, o sea, $\overline{L}_k$ tendría la forma:

	$\overline{Q}^6$		$\overline{Q}^5$		$\overline{Q}^4$		$\overline{Q}^3$		$\overline{Q}^2$		$\overline{Q}^1$		$\overline{Q}^0$
$\overline{L}_k=$	00000	*	00000	*	00000	*	00000	*	00000	1	00000	*	00000	0,

se tendría $\overline{L}_k+\overline{QI}-2\overline{R}_j$, tendría la forma:

$\overline{Q}^6$		$\overline{Q}^5$		$\overline{Q}^4$		$\overline{Q}^3$		$\overline{Q}^2$		$\overline{Q}^1$		$\overline{Q}^0$
00000	*	*****	*	*****	*	*****	*	00001	0	*****	*	*****	*,

lo cual en virtud de (1.62) es un absurdo. De este modo, $\overline{L}_{k,2}=0$, luego la línea que ejecuta $\overline{M}$ en el paso 2 es $\overline{L}i+1$. Por otra parte, $\overline{r}_{j,3}>0$ y $\overline{L}_{i,3}=1$. Esto implica el coeficiente correspondiente a $\overline{Q}^4$ de los números $\overline{QI}-2\overline{R}_j$ y $\overline{QL}_i$ son 0 y 1, respectivamente. Lo cual, por (1.62) obliga a que $\overline{L}_{k,4}=1$, ya que de lo contrario, $\overline{L}_{k,4}=0$, los coeficientes correspondientes a $\overline{Q}^4$ de $\overline{QL}_i$ y $\overline{L}_k+\overline{QI}-2\overline{R}_i$ serían 1 y 0, respectivamente, así (1.62) nos daría una contradicción.

En el razonamiento anterior usamos un hecho fundamental, pero que, en general, queda implícito: siempre que se suman en binaro un número como L_k (cuya descomposición en base Q tiene solo unos y ceros) y un número como $QI-2R_j$ (con $Rj=\sum_{t=0}^{s} r_{j,t}Q^t$ y $0\leq r_{j,t}<Q/2$), los coeficientes de $L_k+QI-2R_i$, correspondientes a potencias de Q, se pueden computar simplemente sumando los correspondientes coeficientes, en binario, de L_k y $QI-2R_i$.

De lo anterior, tenemos que (1.61) implica que $r_{j,t}>0$ si y sólo si $l_{k,t+1}=1$. La razón por la que dividimos Q entre 2, en 1.52, puede ser entendida ahora. Usamos $QI-2R_i$, en lugar de

$I - 2R_i$, para poder garantizar que $QI - 2R_i$ sea un entero no negativo.

Los comandos de la forma $Li\ IF\ Rj = 0, GOTO\ Lk$ serán codificados de manera análoga al anterior (suponiendo de nuevo que $i + 1 \neq k$):

$$QL_i \preccurlyeq L_k + L_{i+1} \text{ y } QL_i \preccurlyeq L_k + QI - 2R_j. \tag{1.63}$$

En este caso, $r_{j,t} = 0 \Leftrightarrow l_{i+1,t+1} = 0 \Leftrightarrow l_{k,t+1} = 1$.

Aunque los comandos de tipo $L_iRj \leftarrow Rj \pm 1$ no son pensados como un comando de transferencia, existe un comando $GOTO$ implícito asociado a ellos, es decir, $GOTO\ Li + 1$. Así, para comandos de esta clase, es decir, para cada línea Li que contenga comandos de este tipo, necesitamos una condición de la forma

$$QL_i \preccurlyeq L_{i+1}. \tag{1.64}$$

Finalmente, debemos incluir para cada registro una ecuación que nos permita asegurar que el contenido del registro Rj en el instante t es igual al t-ésimo coeficiente, en base Q, del número R_j. Estas ecuaciones son conocidas como las ecuaciones de registro:

$$R_1 + yQ^{s+1} = QR_1 + x + \sum_k QL_k - \sum_i QL_i, \tag{1.65}$$

$$R_i = QR_i + \sum_k QL_k - \sum_i QL_i,\ \ (i = 1, 2, \ldots, r)\,. \tag{1.66}$$

Los índices k e i varían sobre las instrucciones del tipo $L_kRj \leftarrow Rj + 1$ y $LiRj \leftarrow Rj - 1$. La ecuación de registro para $R1$ es distinta de las ecuaciones para los otros registros ya que (asumiendo funciones de una variable) $R1$ es el único registro de entrada-salida. Para entender estas ecuaciones, por ejemplo (1.65), fijemos un instante t durante el cómputo, entonces (1.65) significa que $r_{1,0} = x$ y $r_{j,t+1}$ es igual al valor que había en Ri en el instante anterior, o sea, $r_{i,t}$ (el coeficiente correspondiente a Q^{t+1}, del número QRi), más un 1 por cada instrucción $L_kR_i \leftarrow R_i + 1$ (ejecutada antes del instante $t + 1$), más un -1 por cada instrucción $L_iR_i \leftarrow R_i - 1$. Es decir, el valor exacto que debe tener $r_{i,t+1}$. Además, (1.65) también garantiza que para el último paso del cómputo, s, el valor de $r_{1,s}$ sea y.

Cuando más registros son considerados como registros de entrada-salida, es necesario agregar más ecuaciones como (1.65) para estos registros.

Apartir de estas ecuaciones y condiciones, no es dificil demostrar, por inducción en t (el número necesario de pasos para hacer el cómputo), que si la máquina M computa la función f, entonces para cada x, y, las condiciones 1.49, 1.50, 1.51, 1.54, 1.55, 1.56, 1.57, 1.58, 1.59, 1.60, 1.61, 1.63, 1.64, 1.65 y 1.66 tienen solución en las variables $s, Q, I, R1, R2, \ldots, Rr, L1, \ldots, L_{l+1}$, si y sólo si, $f(x) = y$. Los resultados de las secciones anteriores nos permiten escribir todas estas

condiciones como un polinomio diofantino en las variables anteriores y algunas otras. Después de renombrar las variables $x_1, \ldots, x_n$ y transformar todas las relaciones diofantinas en una sola, obtenemos una ecuación polinómica

$$y = f(x) \Leftrightarrow (\exists x_1, x_2, \ldots, x_n) [P(x, y, x_1, x_2, \ldots, x_n) = 0]. \tag{1.67}$$

Cuando f es una función cuyas imagenes son m-tuplas, (1.67) se extiende naturalmente, ya que sólo basta poner m condiciones como (1.65), reemplazando cada yQ^{s+1} por y_iQ^{s+1}(donde $f(x) = (y_1, y_2, \ldots, y_n)$), y eliminando el término x de todas, salvo la primera.

Ahora, demostremos el teorema 1.1.1. Sea $A(a_1, a_2, \ldots, a_n) \neq \emptyset$ un conjunto listable. Entonces A es el rango de una función recursiva f, luego existe una ecuación polinómica $P(x, y_1, \ldots, y_m, x_1, x_2, \ldots, x_n)$ tal que

$$f(x) = (y_1, y_2, \ldots, y_m) \Leftrightarrow (\exists x_1, x_2, \ldots, x_n) [P(x, y_1, y_2, \ldots, y_m, x_1, x_2, \ldots, x_n) = 0].$$

Así,

$$\begin{aligned} A(a_1, a_2, \ldots, a_n) &\Leftrightarrow (\exists x) [f(x) = (a_1, a_2, \ldots, a_n)] \\ &\Leftrightarrow (\exists x, x_1, \ldots, x_n) [P(x, a_1, \ldots, a_m, x_1, x_2, \ldots, x_n) = 0]. \end{aligned}$$

De este modo obtenemos el teorema 1.1.1.

1.6 El décimo problema de Hilbert es insoluble

En esta sección demostraremos que el teorema 1.1.1 implica la insolubilidad del décimo problema de Hilbert, utilizando una idea debida T. Rado. Conocida como el juego de Rado. Consideremos el problema de programar una máquina registradora para que escriba el número más grande posible en el registro $R1$ y se detenga. Supongamos que todos los registros son inicializados en cero. Sea $R(l)$, el número más grande generado de este modo, por una máquina registradora de l líneas y con todos los registros inicializados en cero.

Si nos restringimos a comandos de sustracción seguros, (1.47)-(1.48), y evitamos ciclos infinitos, vemos que $R(l)$ es una función bien definida en l, ya que existe un número finito de máquinas con l líneas en su programa y por lo tanto un número finito de números computados por ellas, al inicializar todos sus registros en cero.

Claramente, $R(1) = 1, R(2) = 2$. Además $R(l) < R(l+1)$, dado que es posible agregar una linea del tipo $R_1 \leftarrow R_1 + 1$, al final de un programa de l líneas.

Ahora, mostraremos que la función $R(l) = y$ crece demasiado rápido, es decir, que no puede ser computada por ninguna función recursiva.

Lema 1.6.1 *Sea f una función recursiva de $\mathbb{N}$ en $\mathbb{N}$. Entonces, para todo l suficientemente grande $f(l) < R(l)$.*

Prueba. Sin pérdida de generalidad podemos suponer que f es una función estrictamente creciente, ya que si no lo fuera podríamos construir otra función f' recursiva y creciente, tal que $f'(x) \geq f(x)$, para $x \in \mathbb{N}$, y así demostrar la afirmación para t', lo cual implicaría $R(l) > f'(l) \geq f(l)$, para l suficientemente grande.

Sea N una máquina registradora, de c líneas, que compute la función f. Sea F la máquina obtenida, a partir de N, agregando el comando $R1 \leftarrow R1 + 1$ al final.

Así, F es una máquina de $c+1$ líneas que computa la función $f(x)+1$. Sea D una máquina registradora de 5 líneas, con la propiedad de que cuando se inicia con x en el registro $R2$ y cero en el registro $R1$, computa $2x$ en el registro $R1$, cero en $R2$ y se detiene. D podría ser la siguiente máquina:

L1 IF $R2 = 0$, GOTO $L6$
$R2 \leftarrow R2 - 1$,
$R1 \leftarrow R1 + 1$,
$R1 \leftarrow R1 + 1$,
GOTO $L1$.

Para cada x, sea M_x una máquina registradora de x líneas con la propiedad de que cuando se inicializa con cero en $R2$ computa x en $R2$ y se detiene. M_x podría consistir en un programa de x líneas de la forma $R2 \leftarrow R2 + 1$.

Consideremos la máquina M_x, seguida de D, seguida de F y denotemosla por $F(D(M_x))$. Esta máquina tiene $x + 6 + c$ líneas en su programa y tiene la propiedad de producir el número $f(2x) + 1$, cuando es inicializada con cero en todos los registros. La existencia de esta máquina prueba que

$$f(2x) \leq R(x + 6 + c), \tag{1.68}$$

para cada x. Cuando $x > 6 + c$, tenemos que $x + 6 + c < 2x$. Luego,

$$f(x + 6 + c) < f(2x), \tag{1.69}$$

ya que f es estrictamente creciente. Ahora, si $l = x+6+c$, entonces para $l > 12+2c\,(x \geq 6 + c)$, (1.68) y (1.69) implican $f(l) > R(l)$. ■

Lema 1.6.2 *No existe un algoritmo para resolver el décimo problema de Hilbert.*

Prueba. Sea $S = \{(k, l) : k \leq R(l)\}$. Entonces, $(k, l) \in S$, si y sólo si, existe una máquina registradora de l líneas, que se detiene en s pasos, (con todos los registros inicializados en cero), que se detiene con un valor en $R1$ mayor o igual a k. De lo anterior se sigue que S es un

conjunto listable. El conjunto S y la función $R(l)$ están relacionados de la siguiente manera:

$$R(l) = \min k\,[(k+1, l) \notin S] \tag{1.70}$$

En virtud del teorema 1.1, existe un polinomio $P(k, l, x_1, x_2, \ldots, x_n)$ con la propiedad

$$(k, l) \in S \Leftrightarrow (\exists x_1, x_2, \ldots, x_n)\,[P(k, l, x_1, x_2, \ldots, x_n) = 0]\,. \tag{1.71}$$

Así de (1.70) y (1.71) tenemos que

$$R(l) = \min k\,[\neg\,(\exists x_1, x_2, \ldots, x_n)\,[P(k, l, x_1, x_2, \ldots, x_n) = 0]]\,.$$

Por lo tanto, si el décimo problema de Hilbert fuera soluble, la función R sería computable, lo cual es absurdo por el lema 1.6.1. ■

A lo largo de los años, los matemáticos se han preocupado por conocer, dada una ecuación diofantina $P = 0$, cotas superiores (relativamente precisas) para el número de soluciones enteras de dicha ecuación. Esta cuestión es igual de compleja que la pregunta hecha por Hilbert en su décimo problema. Para ser más precisos, denotemos por $\#(P)$ al número de soluciones enteras de la ecuación $P = 0$. Así, $0 \leq \#(P) \leq \aleph_0$. Sea $A = \{0, 1, 2, \ldots, \aleph_0\}$. Entonces, si $B \subset A, B \neq \emptyset$ y $B \neq A$, Martin Davis [2] demostró, de manera sencilla y elemental, que no existe un algoritmo para determinar si $\#(P)$ pertenece, o no, a B. Notemos que si $A = \{0\}$, entonces el décimo problema de Hilbert es equivalente a determinar si $\#(P) \in A$, es decir, a determinar si el número de soluciones de la ecuaión es nulo.

Davis logró esta generalización usando, por supuesto, la insolubilidad del décimo problema de Hilbert.

1.7 Algunas consecuencias

Aunque la imposibilidad de encontrar un algoritmo de decisión para ecuaciones diofantinas es un resultado negativo, la solución del problema de Hilbert tiene numerosas consecuencias positivas. Una de ellas es la existencia de polinomios, cuyo conjunto de valores positivos coincide con cualquier conjunto listable A, dado de antemano.

Teorema 1.7.1 *Sea f una función recursiva con valores en los números naturales. Entonces, existe un polinomio diofantino Q tal que para todo par de números naturales x, y se cumple lo siguiente:*

$$f(x) = y \Leftrightarrow (\exists x, x_1, \ldots, x_n)\,[Q(x, x_1, \ldots, x_n) = y]\,.$$

Prueba. Aplicando el teorema 1.1.1 a la gráfica de f, obtenemos una representación diofantina con polinomio P. Ahora, usando un truco de Hilary Putnam y el hecho de que f es

una función no negativa, tenemos que

$$\begin{aligned} f(x) &= y \Leftrightarrow (\exists x_1, x_2, \ldots, x_n)\left[P(x, y, x_1, x_2, \ldots, x_n) = 0\right] \\ &\Leftrightarrow (\exists x_0, x_1, \ldots, x_n)\left[1 - P(x, x_0, x_1, x_2, \ldots, x_n)^2 = 1 \wedge x_0 = y\right] \\ &\Leftrightarrow (\exists x_0, x_1, \ldots, x_n)\left[(x_0 + 1)\left[1 - P(x, x_0, x_1, x_2, \ldots, x_n)^2\right] = y + 1\right] \end{aligned}$$

Así, para $Q(x, x_0, x_1, \ldots, x_n) = (x_0 + 1)\left[1 - P(x, x_0, x_1, x_2, \ldots, x_n)^2\right] - 1$ se cumple el teorema. ■

Si tomamos la función $f(n) = P_n$, donde P_n es el n-ésimo número primo, en el teorema anterior obtenemos un polinomio Q_p, cuyos valores positivos coinciden con el conjunto de los números primos. La prueba del teorema 1.1.1 es constructiva en el sentido en que nos muestra como obtener tal polinomio. Matiyasevich ha construido un polinomio en 10 variables con dicha propiedad, lo cual representa una mejora considerable desde que J.P. Jones, D. Sato, H. Wada y D. Wiens mostraron un polinomio, con la misma propiedad, en 26 variables y de grado 25. La hipotética existencia de un polinomio con la propiedad anterior, prevista por los matemáticos mucho antes de 1970, fue una de las grandes evidencias en contra de la hipotesis de Martin Davis. Este escepticismo era fundamentado por hechos del siguiente estilo: un polinomio $Q(z_1, z_2, \ldots, z_n)$ con coeficientes complejos que tome únicamente valores primos, para valores no negativos de las variables es constante. La prueba de este hecho es completamente elemental, mas no trivial, y se deja como ejercicio al lector interesado. Otro corolario interesante del teorema 1.1.1 es el siguiente: es posible listar la colección de todos los conjuntos r.e. de n-tuplas de números naturales $A_0, A_1, \ldots$En forma precisa, existe un conjunto listable de $n+1$-tuplas U_n tal que

$$(a_1, a_2, \ldots, a_n) \in A_k \Leftrightarrow (a_1, a_2, \ldots, a_n, k) \in U_n.$$

Aplicando el teorema 1.1.1 a este conjunto obtenemos una ecuación diofantina particular P_n con la siguiente propiedad:

$$(a_1, a_2, \ldots, a_n) \in A_k \Leftrightarrow (\exists y_1, y_2, \ldots, y_m)\left[P_n(a_1, a_2, \ldots, a_n, k, y_1, y_2, \ldots, y_m) = 0\right].$$

Así, una representación diofantina de un conjunto arbitrario de n-tuplas se puede obtener tan sólo fijando el valor de una de sus variables. Algo aún más sorprendente es que se puede extender este resultado al caso $n = 0$ y obtener la siguiente forma fuerte de la insolubilidad del décimo problema de Hilbert.

Teorema 1.7.2 *Existe una ecuación diofantina en un parametro*

$$D\left(a, x_0, x_1, \ldots, x_m\right) = 0, \tag{1.72}$$

tal que ningun algoritmo puede resolver el siguiente problema: decidir si la ecuación tiene una solución $x_1, x_2, \ldots, x_m \in \mathbb{N}$*, para cada valor fijo de* a*.*

Así, para obtener indecibilidad no es necesario considerar la clase de todas las ecuaciones diofantinas, es suficiente considerar ecuaciones diofantinas con grado acotado, en un número fijo de variables desconocidas, más aún, obtenidas de un polinomio particular D, tan sólo fijando números en una de sus variables. El hecho empírico de que el nivel de complejidad de una ecuación diofantina crece conforme crecen el número de variables y el grado de la ecuación, podría no ser muy plausible para valores grandes de estos (variables y grados), ya que, en virtud del teorema anterior, la complejidad de una ecuación alcanza un tope para ecuaciones con grado y número de variables acotados. Además, la ecuación

$$P_n\left(a_1, \ldots, a_n, k, y_1, \ldots, y_m\right) = 0, \tag{1.73}$$

podría considerarse como una *ecuación universal* en el siguiente sentido: para cada ecuación diofantina

$$P_n\left(a_1, \ldots, a_n, x_1, \ldots, x_m\right) = 0, \tag{1.74}$$

se puede encontrar, de manera efectiva, un número particular k_p tal que, para valores fijos de los parámetros $a_1, \ldots, a_n$, la ecuación 1.74 tiene solución en $x_1, \ldots, x_n$, si y sólo si, la ecuación

$$P_n\left(a_1, \ldots, a_n, k_p, y_1, \ldots, y_m\right) = 0, \tag{1.75}$$

tiene solución en $y_1, \ldots, y_m$. Esto implica que para efectos de solubilidad, la colección de ecuaciones como (1.74), con grados arbitrariamente grandes, es igual de compleja que la ecuación 1.73, con grado fijo.

Por otra parte, Hilbert también incluyó en su lista de problemas a la famosa *conjetura de Goldbach*. Esta conjetura, aún sin resolver, afirma que cada número par mayor que 2 es la suma de dos números primos. Sea C el conjunto de números pares que son contraejemplo para la conjetura de Goldbach. Evidentemente C es un conjunto recursivo, así, existe una ecuación diofantina $G\left(a, x_1, \ldots, x_n\right) = 0$, la cual tiene solución, si y sólo si, a es un contraejemplo. En otras palabras, *la conjetura de Goldbach es cierta, si y sólo si, la ecuación*

$$G\left(x_0, x_1, \ldots, x_n\right) = 0, \tag{1.76}$$

no tiene soluciones.

Otro teorema interesante, es el último teorema de Fermat. Esta teorema afirma que el sistema infinito de ecuaciones diofantinas

$$x^n + y^n = z^n, \tag{1.77}$$

para $n \geq 3, x \geq 1, y \geq 1$, no tiene soluciones. Si vemos la ecuación 1.76 como una sola ecuación diofantina exponencial en las variables n, x, y, z y usamos el hecho de que la relación exponencial es diofantina, garantizamos la existencia de una ecuación diofantina

$$F(n, x, y, z, u_1, \ldots, u_m) = 0,$$

la cual tiene solución en $u_1, \ldots, u_m$, si y sólo si, n, x, y, z son soluciones de (1.77). De este modo, concluimos que *el último teorema de Fermat es equivalente a que la ecuación*

$$F(n + 3, x + 1, y + 1, z, u_1, \ldots, u_m) = 0$$

no tenga solución en los números naturales.

Finalmente, es posible demostrar que *existe una ecuación diofantina* $R(x_1, \ldots, x_m) = 0$ *la cual no tiene soluciones si y sólo si la Hipótesis de Riemann es cierta. Lo mismo sucede con el problema de los cuatro colores.*

Sin embargo, no es factible que cada problema de las matemáticas sea cierto, si y sólo si, una cierta ecuación diofantina es insoluble. De hecho, se cree que la conjetura de la infinidad de primos gemelos (de diferencia 2) no se puede plantear de este modo.

Una pregunta natural que nos podríamos hacer en este punto sería la siguiente: ¿son estas representaciones diofantinas útiles? Bueno, el décimo problema de Hilbert es insoluble, así que no disponemos de un método universal para todas ecuaciones. Dificilmente podemos comprender las correspondientes ecuaciones diofantinas para estos problemas ya que son bastante complicados. No obstante, podríamos reversar el orden de las cosas o sea el décimo problema es insoluble y tenemos que inventar más y mejores métodos para resolver un número mayor de ecuaciones diofantinas. Esto significa que podríamos ver la prueba del último teorema de Fermat y el problema de los cuatro colores como herramientas muy sofisticadas para decidir sobre ecuaciones diofantinas particulares y tratar de extender estas técnicas a otras ecuaciones. Las reducciones anteriores de problemas famosos a ecuaciones diofantinas podrían tomarse como una razón empírica de porqué el décimo problema de Hilbert es indecidible, es decir, dificilmente se podría esperar que tantos problemas, tan dificiles y de areas distintas de las matemáticas, pudieran ser atacados mediante un método mecanico universal.

Capítulo 2

ALGUNAS EXTENSIONES

2.1 Terminología y otros preliminares

En esta sección recordaremos algunas nociones y resultados fundamentales de la lógica matemática los que usaremos a lo largo del resto de esta monografía. Para un tratamiento riguroso de los hechos mencionados a continuación recomendamos el libro de David Marker [11].

Informalmente, una *fórmula de primer orden* en el lenguaje de anillos $(0, 1, +, \cdot)$ es una expresión construida a partir de los símbolos $+, \cdot, 0, 1, =, ()$, las relaciones $\wedge$ (conjunción), $\vee$ (dijunción), $\neg$ (negación), los cuantificadores $\forall$ (universal), $\exists$ (existencial), y variables $x, y, z, \ldots$ Para ser un poco más precisos, primero se definen los *términos*, que en nuestro caso, son simplemente expresiones formales construidas a partir de las variables por medio de las operaciones $+, \cdot$. Luego, se definen las *fórmulas atómicas*, las cuales son expresiones de la forma $t_1 = t_2$, donde t_1, t_2 son términos. En el caso general, donde el lenguaje contiene símbolos para relaciones R^N de variables, expresiones de la forma $R^N(t_1, t_2, \ldots, t_N)$, donde $t_1, t_2, \ldots, t_N$ son términos, también se consideran como expresiones atómicas. Sin embargo, en nuestro trabajo éstas no aparecerán. Continuando con lo anterior, se define el conjunto de fórmulas de primer orden como el menor conjunto W que contiene a las fórmula atómicas tal que:

1. Si ϕ está en W, entonces $\neg\phi$ está en W.

   Si ϕ y ψ están en W, entonces $(\phi \wedge \psi)$ y $(\phi \vee \psi)$ están en W.

   Si ϕ está en W y x_i es una variable, entonces $(\forall x_i \phi)$ y $(\exists x_i \phi)$ están en W.

Decimos que una variable x_i es *libre* en una fórmula ϕ , si esta no está dentro del alcance de un cuantificador $\forall$ o $\exists$. En caso contrario decimos que la variable es ligada. Por ejemplo en la siguiente fórmula x_3 y x_4 son las dos únicas variables libres:

$$\phi \equiv (\forall x_1)(\exists x_2)((x_1 \cdot x_3 = x_4 + x_2) \vee \neg(x_3 \cdot x_3 \cdot x_3 = 1)).$$

Una sentencia de primer orden es una fórmula de primer orden (o fórmula, para simplicar) que no tiene varibales libres.

Notemos que cualquier ecuación diofantina $P(x_1, \ldots, x_n) = 0$ es equivalente a una fórmula. Por ejemplo, la ecuación $x_3 \cdot x_2 - x_1 + x_3 - x_4 \cdot x_1 = 0$ es equivalente a la fórmula $x_3 \cdot x_2 +$

$x_3 = x_1 + x_4 \cdot x_1$. La idea es simplemente pasar al lado derecho de la ecuación diofantina los términos del lado izquierdo que tienen signo negativo. De ahora en adelante no haremos ninguna diferencia entre una ecuación diofantina y su representante.

Una *inecuación diofantina* es una expresión de la forma $D(x_1, \ldots, x_n) \neq 0$, donde $D(x_1, \ldots, x_n)$ es un polinomio diofantino. Es importante notar que en algunos casos nuestro lenguaje incluirá un número finito de símbolos adicionales para ciertas constantes destacadas (dependiendo del anillo particular que estamos considerando), y así la definición de ecuación (inecuación) se extiende a esta situación de manera natural, con la única diferencia de que los coeficientes de la ecuación estarán en este caso en el subanillo más pequeño que contenga a $0, 1$ y a todas las constantes elegidas.

Una fórmula de la forma

$$(\exists x_1) \ldots (\exists x_n) S, \tag{2.1}$$

donde S es la dijunción de sistemas de ecuaciones e inecuaciones difoantinas (en principio (2.1) puede tener más variables que $x_1, \ldots, x_n$) se llamará *fórmula existencial*. Si S no contiene inecuaciones, entonces (2.1) se llamará fórmula *positivamente existencial*. Además, en el caso particular en el que S sea una sola ecuación diofantina, (2.1) se llamará una *fórmula diofantina*.

Sea R un anillo conmutativo con unidad. Una vez fijado el lenguaje, una sentencia tendrá un *valor de verdad*, definido del modo usual, haciendo que las variables tomen valores en R. Cuando $\phi(x_1, \ldots, x_n)$ es una fórmula (con variables libre $x_1, \ldots, x_n$) sólo se podrá obtener un valor de verdad para $\phi(a_1, \ldots, a_n)$ reemplazando las variables $x_1, \ldots, x_n$, por $a_1, \ldots, a_n \in R$. Dada una fórmula ϕ, con n variables libres, ésta define un subconjunto de R^n, es decir, el conjunto

$$A_\phi = \{\overline{a} \mid \phi(a_1, \ldots, a_n) \text{ es cierta en } R\}. \tag{2.2}$$

Definición 2.1.1 *Un subconjunto definido por (2.2), donde ϕ es una fórmula (respectivamente fórmula existencial, positivo-existencial, diofantina) sobre R se llama conjunto definible (respectivamente existencial, positivo-existencial, diofantino).*

A continuación mostraremos que bajo ciertas hipótesis sobre el anillo R, la clase de los conjuntos positivo-existenciales coincide con la clase de los conjuntos diofantinos sobre R.

Proposición 2.1.1 *Sea R un anillo par el que existen polinomios $f(x, y), g(x, y) \in R[x, y]$ tales que para $a, b \in R$ se cumple que*

$$f(a, b) = 0 \Leftrightarrow a = 0 \wedge b = 0, \tag{2.3}$$

$$g(a, b) = 0 \Leftrightarrow a = 0 \vee b = 0. \tag{2.4}$$

Si el lenguaje tiene suficientes símbolos para elementos que puedan expresar a los coeficientes de f y g como combinaciones de estos, entonces la colección de conjuntos positivo-existenciales coincide con la colección de conjuntos diofantinos sobre R.

Prueba. La contención interesante es mostrar que los conjuntos positivo-existenciales son diofantinos. Dada una fórmula positivo-existencial, la transformamos inductivamente en una fórmula diofantina, definiendo el mismo conjunto, repitiendo las siguientes operaciones: *a*) $(p = 0) \wedge (q = 0)$ lo reeplazamos por $f(p, q) = 0$;

b) $(p = 0) \vee (q = 0)$ lo reemplazamos por $g(p, q)$. De este modo se obtiene la proposición. ■

Cuando R es un dominio se puede construir un polinomio, con la propiedad 2.4 de manera trivial: $g(x, y) = xy$.

Ahora, veamos que si el campo de funciones de R no es algebraicamente cerrado, podemos construir un polinomio con la propiedad 2.3. En efecto, sea $f(x) \in K(R)[x]$ un polinomio que no tenga raíces en $K(R)$. Después de multiplicar por un factor adecuado podemos suponer que $f(x) \in R[x]$. Sea $h(x, y) = y^d f\left(\frac{x}{y}\right)$, la homogenización de f (donde d es el grado de f). Es un ejercicio elemental probar que para cada $a, b \in R$ se tiene que $h(a, b) = 0 \Leftrightarrow a = 0 \wedge b = 0$.

Por otra lado, las fórmulas de primer orden son reconocibles o codificables por una máquina registradora (o máquina de Turing), lo cual le da sentido a la siguiente definición.

Definición 2.1.2 *La teoría de primer orden o teoría, (respectivamente teoría existencial, positivo-existencial, diofantina) en el lenguaje de anillos (posiblemente con finitos símbolos adicionales para constantes) es el conjunto de sentencias de primer orden (respectivamente sentencias existenciales, positivo-existenciales, diofantinas) que son verdaderas cuando las variables se mueven en R. La teoría (respectivamente teoría existencial, positivo-existencial, diofantina) es* decidible o soluble *si existe una máquina de Turing que toma como entrada una sentencia de primer orden (respectivamente teoría existencial, positivo-existencial, diofantina) y decide si pertenece o no a la teoría (respectivamente teoría existencial, positivo-existencial, diofantina).*

Es importante notar que cuando el lenguaje contiene símbolos adicionales para elementos destacados del anillo, (por ejemplo, un símbolo adicional "t") es necesario que haya una codificación fija del anillo generado por $0, 1$ y los símbolos que se agregaron (que actuarán como indeterminadas) para que la máquina de Turing pueda reconocer las sentencias de primer orden. Éste es básicamente un problema técnico que puede resolverse introduciendo la noción de *anillo recursivo*.

Un anillo conmutativo con unidad R es recursivo si existe una biyección $\theta : \mathbb{N} \to R$ tal que

las funciones

$$\begin{aligned} S &: \mathbb{N}\times\mathbb{N}\to\mathbb{N} : (n,m)\to\theta^{-1}\left[\theta(n)+\theta(m)\right], \\ M &: \mathbb{N}\times\mathbb{N}\to\mathbb{N} : (n,m)\to\theta^{-1}\left[\theta(n)\cdot\theta(m)\right], \end{aligned}$$

son recursivas. La función θ se puede interpretar como la codificación o indexación del anillo R en el universo de las máquinas de Turing, y la recursividad de las funciones S y M significan que si se tiene los códigos e índices de los elementos $a_n, a_m \in R$, entonces se pueden computar los índices de $a_n + a_m$ y $a_n \cdot a_m$. Notemos que los codigos de los elementos 0 y 1 se pueden averiguar de manera efectiva ya que son los unicos números naturales a_0 y a_1 tales que $S(a_0, a_0) = a_0$ y $M(a_1, a_1) = a_1$, respectivamente.

Esta noción permite extender definiciones de la lógica a subconjuntos de R^n, como por ejemplo, la noción de listabilidad. Es decir, un conjunto $F \subseteq R^n$ es listable si el conjunto $\overline{F} \subseteq \mathbb{N}^n$, definido como

$$(k_1,\ldots,k_n)\in\overline{F} \Leftrightarrow (\exists x_1,\ldots,x_n\in R)\left[(x_1,\ldots,x_m)\in F \wedge x_i=\theta(k_i)\right],$$

es listable.

Es un ejercicio elemental, aunque algo engorroso, demostrar que el anillo $\mathbb{Z}[t]$ *es un anillo recursivo*. De hecho, es posible mostrar que si R es recursivo entonces $R[t]$ lo es. Anillos del tipo $\mathbb{Z}[t_1,\ldots,t_n]$ son los que aparecen naturalmente como coeficientes de las ecuaciones diofantinas cuando agregramos finitos elementos $t_1,\ldots,t_n$ al lenguaje de anillos. Los hechos anteriores se dejan como ejercicios al lector, ya que su demostración formal tomaría varias paginas y no tendría ninguna trascendencia para el trabajo que estamos realizando. Es importante notar que si R es un anillo recursivo (con una indexación ϕ fija) y se define sobre él otra indexación ψ, entonces siempre se puede construir una máquina de Turing que decodifique una indexación en la otra.

Ahora, pasamos a definir el décimo problema de Hilbert sobre un anillo conmutativo con unidad R.

Definición 2.1.3 *Sea R un anillo conmutativo con unidad.*

1) *El décimo problema de Hilbert sobre R ($H10(R)$) pide encontrar un algoritmo con entrada y salida de la siguiente manera:*

Entrada: $f \in \mathbb{Z}[x_1,\ldots,x_n]$

Salida: "sí" o "no", dependiendo de si se cumple que exista un n-tupla $(t_1,\ldots,t_n)\in R^n$ tal que $f(t_1,\ldots,t_n)=0$. (existe un único homomorfismo de anillos $h:\mathbb{Z}\to R$ que le da sentido a evaluar a f en elementos de R).

2) *Si $S \subseteq R$, entonces el décimo problema de Hilbert sobre R, con coeficientes en S*

($H10_S(R)$) *es el mismo que en 1, con la única diferencia que los coeficientes de* f *están en* S *en lugar de estar en* $\mathbb{Z}$. *Aquí suponemos que una codificación para* S *ha sido especificada.*

Es importante resaltar que debido a la existencia de máquinas de Turing $M_{\phi\psi}$ para codificar una indexación ϕ en otra ψ y viceversa, el décimo problea de Hilbert sobre R con coeficientes en S está bien definido, ya que si existe una máquina de Turing M_ϕ para resolver $H10_S(R)$ con respecto a ϕ, entonces la maquina de Turing $M_{\psi\phi}M_\phi M_{\phi\psi}$ (esto significa la máquina $M_{\phi\psi}$, seguida de M_ϕ y seguida de $M_{\psi\phi}$) resuelve $H10_S(R)$ con respecto a ψ. Es decir, si se nos diera una ecuación codificada por ψ, entonces la traducimos a la codificación ϕ, decidimos si es soluble o no y luego traducimos de nuevo la respuesta al código ψ. Por simetría tenemos que $H10_S(R)$ es soluble con respecto a ϕ si y sólo si es soluble con respecto a ψ.

Para terminar esta sección enunciaremos algunos resultados clásicos que serán de mucha utilidad a lo largo de este capítulo.

Las teorías sobre $\mathbb{N}$ y $\mathbb{Z}$ (denotadas por $T(\mathbb{N})$ y $T(\mathbb{Z})$, respectivamente) son indecidibles (Gödel, Church, Rosser, 1930-40). De hecho, estos resultados son implicados por la insolubilidad de $H10(\mathbb{N})$ y $H10(\mathbb{Z})$ ya que ni siquiera existe un algoritmo para decidir sobre sentencias diofantinas. En su tesis doctoral Julia Robinson demostró, entre otras cosas, que $\mathbb{Z}$ era definible en $\mathbb{Q}$. Su demostración se basa en la aritmética de las formas cuadráticas en 3 variables. Ahora, supongamos que $\phi(x)$ es una fórmula que define a $\mathbb{Z}$ en $\mathbb{Q}$. Entonces, si la teoría $T(\mathbb{Q})$ fuera soluble, la teoría $T(\mathbb{Z})$ lo sería ya que dada una sentencia ψ (con variables $x_1, \ldots, x_n$), tendríamos que ψ es cierta en $\mathbb{Z}$, si y sólo si, $\psi \wedge \phi(x_1), \ldots, \phi(x_n)$ es cierta en $\mathbb{Q}$. Así, dicho algoritmo decidiría sobre sentencias en $\mathbb{Z}$. Cuando al referirnos a una teoría $T(R)$ no mencionemos el lenguaje, es porque se sobreentendrá que éste es $(0, 1, +, \cdot)$.

2.2 Rudimentos sobre curvas elípticas

En la sección siguiente veremos como se pueden usar algunos hechos básicos de la teoría de las curvas elípticas para probar insolubilidad de teorías lógicas. Para hacer este trabajo autocontenido, daremos una explicación de las nociones y propiedades más elementales de las curvas elípticas que se usarán más adelante. Se recomienda al lector la consulta de cualquiera de los libros clásicos [25] y [26].

Definición 2.2.1 *Una curva elíptica sobre* $\mathbb{Q}$ *es una curva en* $\mathbb{R}^2$ *definida por*

$$E = \left\{(x, y) \in \mathbb{R}^2 \mid y^2 = ax^3 + bx^2 + cx + d\right\},$$

donde $a, b, c, d \in \mathbb{Q}$ *y la ecuación cúbica* $ax^3+bx^2+cx+d = 0$ *no tiene raíces múltiples. Además definimos*

$$E(\mathbb{Q}) = \left\{(r, s) \in \mathbb{Q}^2 \mid s^2 = ar^3 + br^2 + cr + d\right\} \cup \{\infty\}.$$

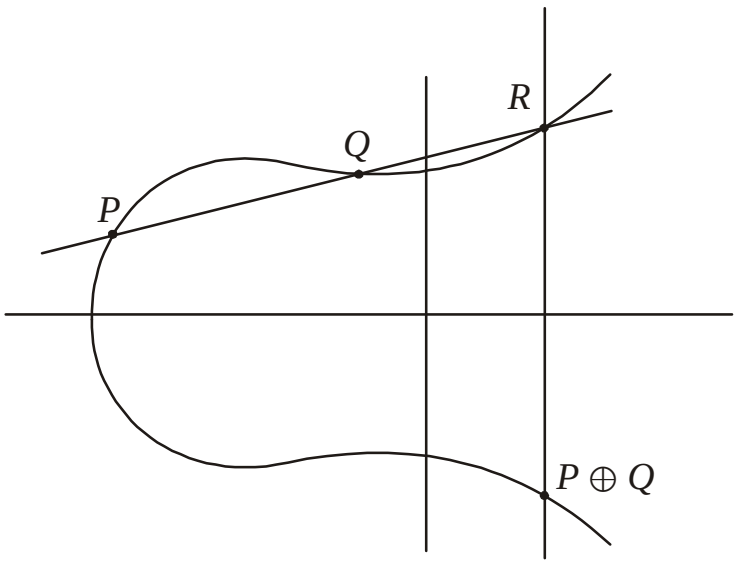

Figura 2-1: $P \oplus Q$

Aquí, ∞ es un símbolo que representa el "punto en el infinito".

Es posible definir una operación binaria $\oplus$ que dota a $E(\mathbb{Q})$ de estructura de grupo abeliano, de la siguiente manera: ∞ es por definiciónel elmento neutro del grupo. Si $P, Q \in E(\mathbb{Q}), P \neq \infty, Q \neq \infty, P \neq Q$ y $R(x, y)$ es el tercer punto de intersección de la curva elíptica con la línea l que une a P con Q. Definimos $P \oplus Q = (x, -y)$. Ver Figura 2-1. Si $P = Q, P \neq \infty, Q \neq \infty$, entonces se puede probar (usando el hecho de que la cúbica tiene todas sus raíces distintas) que la recta tangente a la curva elíptica en el P corta a la curva elíptica en exactamente otro punto $R(x, y)$; luego definimos $2P = P \oplus P = (x, -y)$.

La operación $\oplus$ es algebraica, es decir, las coordenadas de $P \oplus Q$ vienen dadas por funciones racionales (con coeficientes en $\mathbb{Q}$) en las coordenadas de P y Q. Las fórmulas explícitas se pueden consultar en [26]. Usando dichas fórmulas se prueba que la operación $\oplus$ es conmutativa y asociativa, así que $(E(\mathbb{Q}), \oplus)$ es un grupo abeliano. Notemos que si $F \subseteq \mathbb{C}$ es un campo, podemos considerar las soluciones a la ecuación cúbica que define a la curva E con coordenadas en F, $E(F)$. De lo anterior se sigue que la operación $\oplus$ viene dada por funciones racionales con coeficientes en $\mathbb{Q}(F)$ en las componentes de los puntos. En consecuencia

$$E(F) = \left\{(r, s) \in F^2 \mid s^2 = ar^3 + br^2 + cr + d\right\} \cup \{\infty\},$$

es, del mismo modo, un grupo abeliano. En particular, $E(\mathbb{R})$ lo es. Por ejemplo, para la curva

$$E_0 = \left\{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 - 4\right\},$$

la operación $\oplus$ viene dada de la siguiente manera: si $P=(x_1,y_1), Q=(x_2,y_2)$ pertenecen a la curva E_0, entonces

$$2P=\left(\frac{1}{4y_1^2}\left(4x_1^4+32x_1\right),\frac{1}{8y_1^3}\left(x_1^6-80x_1^3-128\right)\right)$$

y si $x_1\neq x_2$,

$$P\oplus Q=\left(\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2,\left(\frac{y_2-y_1}{x_2-x_1}\right)x_3+\frac{y_2x_1-y_1x_2}{x_2-x_1}\right).$$

El punto $(2,2)\in E(\mathbb{Q})$. Calculando con las fórmulas tenemos que

$$2P=(5,-11),3P=\left(\frac{106}{9},\frac{1090}{27}\right),-P=(2,-2)$$

y $-2P=(5,11)$ (Fermat logró demostrar que las únicas soluciones enteras son $(2,\pm 2)$ y $(5,\pm 11)$).

2.3 La teoría sobre $\mathbb{Q}(t)$

En esta sección mostraremos una aplicación de las curvas elípticas al problema de probar la insolubilidad de la teoría $T(\mathbb{Q}(t))$, donde $\mathbb{Q}(t)$ es el campo de fracciones del anillo de polinomios, en la variable t, con coeficientes en $\mathbb{Q},\mathbb{Q}[t]$. Esta aplicación fue descubierto por primera vez por Rafael Robinson. La curva elíptica que usaremos será E_0, que definimos en la sección anterior. Primero demostremos varios lemas sobre esta curva.

Lema 2.3.1 *$E_0(\mathbb{Q})$ es un subconjunto infinito y denso en $E_0(\mathbb{R})$.*

Prueba. Sea $r\in\mathbb{Q}, r=\frac{m}{n},(m,n)=1$. Entonces definimos el tamaño de $r, t(r)$ como:

$$t(0)=1 \text{ y } t(r)=\max\{|m|,|n|\}.$$

Si $P\in E(\mathbb{Q})$, entonces definimos $t(P)=t(x)$, donde $P=(x,y)$ y $t(\infty)=0$. Vamos a mostrar que para ciertos puntos P el tamaño de $2P$ es mucho mayor que el tamaño de P. Supongamos que $P=\left(\frac{m}{n},y\right)$ con $m,n\in\mathbb{Z},(m,n)=1$. Así, la primera coordenada de $2P$ es $\frac{\left(m^3+32n^3\right)m}{4n\left(m^3-4n^3\right)}$. Supongamos además, que elegimos a P de tal modo que m es impar. Luego, es claro que $\left(4n,\left(m^3+32n^3\right)m\right)=1$, lo cual implica que cualquier cancelación entre el numerador y el denominador de la primera coordenada de $2P$ no afecta al factor $4n$. Por lo tanto, $t(2P)\geq 4|n|$ y el numerador de la primera coordenada de $2P$ sigue siendo par. Así, por

una inducción trivial obtenemos

$$t\left(2^k P\right) \geq 4^k, k = 1, 2, \ldots,$$

lo cual implica inmediatamente que la sucesión $P, 2P, \ldots$, tiene infinitos puntos. Sólo falta elegir a P, definámoslo como $P = (5, 11)$. De este modo, no sólo hemos probado que $E(\mathbb{Q})$ es infinito, si no también que el grupo generado por el punto $-P = (2, 2)$ es isomorfo a $\mathbb{Z}$. Por otra parte, un resultado que no probaremos aquí, (y que pertenece a un primer curso de curvas elípticas) es el hecho de que el grupo abeliano $E(\mathbb{Q})$ es topológicamente isomorfo al grupo $\mathbb{R}/\mathbb{Z}$. Donde al punto en el infinito ∞ le corresponde $\overline{0} \in \mathbb{R}/\mathbb{Z}$. De este modo, al elemento $(2, 2)$ le corresponde un número irracional α, ya que de corresponderle un número racional $\frac{m}{n}, (m, n) = 1$, la clase de este número en $\mathbb{R}/\mathbb{Z}$ tendría orden n $\left(\overline{n}.\frac{\overline{m}}{\overline{n}} = \overline{m} = \overline{0} \in \mathbb{R}/\mathbb{Z}\right)$ lo cual es absurdo dado que $(2, 2)$ no tiene orden infinito. Ahora, es un hecho general que si x es un número irracional, entonces el conjunto

$$A = \{m\alpha + n \mid m, n \in \mathbb{Z}\}$$

es denso en $\mathbb{R}$. En efecto, es suficiente probar, dado que A es un grupo, que para cada $\varepsilon > 0$, existe un $\beta \in A$, tal que $0 < \beta < \varepsilon$. Sea $\varepsilon > 0$ fijo. Tomemos un $\gamma \in A$, de tal manera que $0 < \gamma < 1$ (γ podria ser $\alpha - \lfloor \alpha \rfloor$) . Luego, existe un único $n_0 \in \mathbb{N}$ tal que

$$\frac{1}{n_0 + 1} < \gamma < \frac{1}{n_0}. \tag{2.5}$$

Así, multiplicando por $-n_0$ y sumando 1 en 2.5, obtenemos

$$0 < 1 - n_0\gamma < \frac{1}{n_0 + 1},$$

y de este modo obtenemos un número $1 - n_0\gamma \in A$ estrictamente menor que $\frac{1}{n_0 + 1}$, luego haciendo $\gamma_0 = 1 - n_0\gamma$ y aplicando el procedimiento anterior a γ_0, construimos un $\gamma_2 \in A$ y un $n_1 > n_0, n_1 \in \mathbb{N}$, tales que $\gamma_2 < \frac{1}{n_1 + 1}$. Procediendo de manera inductiva construimos una sucesión $(\gamma_n)_{n \in \mathbb{N}}, \gamma_n \in A, \gamma_n > 0$, la cual tiende a cero cuando n tiende a infinito. Lo anterior implica que existe $m \in \mathbb{N}$ tal que $0 < \gamma_m < \varepsilon$, y por lo tanto, A es denso en $\mathbb{R}$. De esto se deduce inmediatamente que $\langle \overline{\alpha} \rangle = \overline{A}$ es denso en $\mathbb{R}/\mathbb{Z}$. Así, $\langle (2, 2) \rangle$ es denso en $E(\mathbb{R})$, y como $\langle (2, 2) \rangle \subseteq E(\mathbb{Q})$, obtenemos la segunda parte del lema. ■

La prueba del siguiente lema es sencilla y se deja como ejercicio al lector.

Lema 2.3.2 *Sea K un campo de característica cero y $\alpha \neq 0$ en K. Entonces se cumple los siguiente:*

i) Si $a, b \in K$ *satisfacen la ecuación* $a^3 + b^3 = \alpha$, *entonces* $x = \dfrac{12\alpha}{a+b}, y = 36\alpha\left(\dfrac{a-b}{a+b}\right)$ *satisfacen la ecuación* $y^2 = x^3 - 2^4 3^3 \alpha^2$.

ii) Si $x, y \in K$ *satisfacen la ecuación* $y^2 = x^3 - 2^4 3^3 \alpha^2$, *entonces* $a = \dfrac{36\alpha + y}{6x}, b = \dfrac{36\alpha - y}{6x}$ *satisfacen la ecuación* $a^3 + b^3 = \alpha$.

En lenguaje geométrico, el lema 2.3.2 está afirmando que las curvas $a^3 + b^3 = \alpha$ y $y^2 = x^3 - 2^4 3^3 \alpha^2$ son *biracionalmente equivalentes.*

Lema 2.3.3 *Sea* K *un campo de característica cero y* $\alpha \neq 0$ *en* K. *Si* $f, g \in K(t)$ *satisfacen* $f^2 + g^2 = \alpha$, *entonces* $f, g \in K$.

Prueba. Sean $f, g \in K(t)$ tales que $f^3 + g^3 = \alpha$. Entonces, multiplicando por un factor adecuado y cancelando factores iguales en la ecuación anterior, sabemos que existen polinomios $p, q, r \in K[t]$, primos entre si, de grados d_p, d_q, d_r, respectivamente, tales que

$$p^3 + q^3 - \alpha r^3 = 0. \tag{2.6}$$

Derivando formalmente esta ecuación obtenemos

$$p'p^2 + q'q^2 - \alpha r'r^2 = 0. \tag{2.7}$$

Ahora, considerando las ecuaciones como un sistema líneal homogéneo

$$\begin{bmatrix} p & q & -\alpha r \\ p' & q' & -\alpha r' \end{bmatrix} \begin{bmatrix} p^2 \\ q^2 \\ r^2 \end{bmatrix} = 0,$$

obtenemos que p^2 divide a $qr' - rq'$, q^2 divide a $rp' - pr'$ y r^2 divide a $pq' - qp'$. Además, si $qr' - rq' = 0$, por ejemplo, entonces dado r y q coprimos se tendría que $q|q'$ y $r|r'$, luego $q, r \in K$, y por lo tanto, $p \in K$. Así, $qr' - rq' \neq 0$, y análogamente $rp' - pr'$ y $pq' - qp'$ son nulos. De lo anterior, comparando grados, obtenemos que si alguno de los polinomios p, q o r fuera no constante, se tendría que

$$\begin{aligned} 2d_p &\leq d_q + d_r - 1, \\ 2d_q &\leq d_p + d_r - 1, \\ 2d_r &\leq d_p + d_q - 1, \end{aligned}$$

Sumando estas tres desigualdades obtendríamos que

$$2(d_q + d_q + d_r) \leq 2(d_p + d_q + d_r) - 3,$$

lo cual es absurdo. Así, $r, p, q \in K$, de lo que concluimos la validez el lema. ■

Lema 2.3.4 *Si $f, g \in \mathbb{R}(t)$, satisfacen $f^2 = g^3 - 4$, entonces $f, g \in \mathbb{R}$.*

Prueba. Sea $\alpha = \dfrac{1}{6\sqrt{3}}$, es decir, $4 = 2^4 3^3 \alpha^2$. Aplicando el lema 2.3.3 y la segunda parte del lema 2.3.2, obtenemos que $a, b \in \mathbb{R}$, donde

$$a = \frac{36\alpha + f}{6g}, b = \frac{36\alpha - f}{6g},$$

pero

$$a = \frac{36\alpha - f}{6g} + \frac{2f}{6g} = b + \frac{2f}{6g},$$

luego $\dfrac{f}{g} = 3(a - b)$ es un constante distinta de cero, ya que $a - b = 0$ implica que $f = 0$ y $g = \sqrt[3]{4}$, y en ese caso se cumple el lema.

De lo anterior tenemos que existe un $r \in \mathbb{R}$ tal que $f = rg$. Sea $g = \dfrac{h}{s}$, donde $h, s \in \mathbb{R}[t]$,con h y s son coprimos. Así, de la ecuación original tenemos que $r^2 s h^2 = h^3 - 4s^3$, de lo cual concluimos que s divide a h y h divide a s. Esto, junto con la coprimalidad de h y s significa que $s, h \in \mathbb{R}$, y por lo tanto, $f, g \in \mathbb{R}$. ■

A continuación enunciaresmos un corolario trivial del lema 2.3.4 que usaremos posteriormente en la prueba de la insolubilidad de teoría $T(\mathbb{Q}(t))$.

Corolario 2.3.5 *Si $f, g \in \mathbb{Q}(t)$, satisfacen $f^2 = g^3 - 4$, entonces $f, g \in \mathbb{Q}$.*

Teorema 2.3.6 *La teoría $T(\mathbb{Q}(t))$ es insoluble.*

Prueba. Dado que la teoría $T(\mathbb{Q})$ es insoluble, es suficiente demostrar que $\mathbb{Q}$ es definible en $\mathbb{Q}(t)$. Primero notemos que el teorema de Lagrange se extiende trivialmente a números racionales no negativos, es decir, si $q \in \mathbb{Q}^+$, entonces existen $q_1, q_2, q_3, q_4 \in \mathbb{Q}$ tales que $q = q_1^2 + q_2^2 + q_3^2 + q_4^2$.

Para $x, y \in \mathbb{Q}(t)$ definimos

$$x \geq y \Leftrightarrow (\exists w_1, w_2, w_3, w_4)\left[x - y = w_1^2 + w_2^2 + w_3^2 + w_4^2\right].$$

Observemos que si $x, y \in \mathbb{Q}$, entonces $x \geq y$ coincide con el orden de $\mathbb{Q}$. También definimos $ord(y)$ para $y \in \mathbb{Q}(t)$ como

$$ord(y) \Leftrightarrow (\exists x \in \mathbb{Q}(t))\left[y^2 = x^3 - 4\right].$$

Por el corolario 2.3.5, sabemos que si $ord(y)$ es cierto, entonces $y \in \mathbb{Q}$. Por otra parte, del lema 2.3.1 tenemos que el conjunto $\{y \in \mathbb{Q} / ord(y)$ es cierto$\}$ es denso en $\mathbb{Q}$. Por último, para

$r \in \mathbb{Q}(t)$ definimos

$$con(r) \Leftrightarrow \forall y\,(ord(y) \Leftrightarrow (r \geq y) \vee (y \geq r)).$$

Veamos que $cor(r)$ es cierta, si y sólo si, $r \in \mathbb{Q}$. Sea $r \in \mathbb{Q}$. Entonces, en virtud de $ord(y) \Rightarrow y \in \mathbb{Q}$, tenemos que $con(r)$ es verdadera. Recíprocamente, supongamos por el absurdo que $con(r)$ es cierta para algún $r \in \mathbb{Q}(t) \setminus \mathbb{Q}$. Sabemos, por el teorema del valor intermedio que la imagen de la función no constante r contiene un intervalo de la forma (a, b), de modo que para cualquier número racional $q \in (a, b), r \geq q$ y $q \geq r$ son falsas, debido a que las funciones no constantes $r - q$ y $q - r$ toman valores negativos. Ahora, por la densidad de ord en $\mathbb{Q}$, podemos elegir $s \in \mathbb{Q} \cap (a, b)$ tal que $ord(s)$ es cierta, lo cual implica que $con(r)$ no es cierta.

De lo anterior concluimos que $\mathbb{Q}$ es definible aritméticamente dentro de $\mathbb{Q}(t)$ y así la teoría $T(\mathbb{Q}(t))$ es insoluble. ■

La idea de la demostración es bastante simple y elegante: el grupo $E(\mathbb{Q}(t))$ es igual a $E(\mathbb{Q})$. Las segundas coordenadas de los puntos de la curva definen un subconjunto denso de $\mathbb{Q}$. Y si una función racional es comparable con cada uno de estos números, entonces debe ser constante.

T. Pheidas [17] ha logrado demostrar que $F(t)$ tiene teoría insoluble si F es un campo de característica mayor o igual que 5. Su demostración usa curvas elípticas, pero en este caso, la herramienta útil es el grupo de endomorfismos de la curva.

2.4 La teoría diofantina de $K\left[t, t^{-1}\right]$

En esta sección mejoraremos el resultado obtenido por Pheidas en [18] acerca de la insolubilidad de la teoría existencial sobre $F\left[t, t^{-1}\right]$ y probraremos que la teoría diofantina es indecidible, es decir que $H10_{\mathbb{Z}[t]}\left(F\left[t, t^{-1}\right]\right)$ es insoluble. Aquí F es un campo de característica cero y $F\left[t, t^{-1}\right]$ es el anillo de polinomios en las variables t y t^{-1}, con coeficientes en K. Antes de esto, probaremos varios lemas.

Lema 2.4.1 *Para $x \in F\left[t, t^{-1}\right]$, x es una potencia de $t, x = t^n$, con $n \in \mathbb{Z}$, si y sólo si, x dividide a 1 y $t - 1$ divide a $x - 1$ en $F\left[t, t^{-1}\right]$.*

Prueba. Primero notemos el siguiente hecho elemental que será usando implícitamente en las demostraciones de los lemas de esta sección: sean $y, z \in F\left[t, t^{-1}\right]$ tales que su producto yz es un monomio, es decir un polinomio de la forma αt^m, con $\alpha \in F$ y $m \in \mathbb{Z}$, entonces y y z son también monomios. La prueba de este hecho es sencilla (de hecho es suficiente con que K sea un dominio) y se deja como ejercicio al lector interesado.

Supongamos que $x = t^n$, para algún $n \in \mathbb{Z}$, luego $xt^{-n} = 1$, así $x|1$, además si $n > 0$ se tiene que

$$t - 1 | x - 1 = t^n - 1 = (t - 1)\left(t^{-n-1} + \cdots + 1\right),$$

y si $n < 0$, entonces

$$x-1=\left(t^{-1}\right)^{-n}-1=\left(t^{-1}-1\right)\left(t^{-n-1}+\cdots+1\right)=-\left(t-1\right)t^{-1}\left(t^{-n-1}+\cdots+1\right),$$

así $t-1|x-1$. Recíprocamente, supongamos que $x|1$ y $t-1|x-1$, luego existen $f\left(t,t^{-1}\right), g\left(t,t^{-1}\right) \in K\left[t,t^{-1}\right]$ tales que

$$1=xf\left(t,t^{-1}\right) \text{ y } x-1=\left(t-1\right)g\left(t,t^{-1}\right).$$

La primera condición implia que $x=\alpha t^n$, para algún $\alpha \neq 0$ en F y algún $m \in \mathbb{Z}$. Ahora, de la segunda condición tenemos que $x=\left(t-1\right)g\left(t,t^{-1}\right)+1$, por lo tanto, si evaluamos $t=1$, obtenemos que $x\left(t,t^{-1}\right)=1$, así $\alpha=1$ y $x=t^m$, como se quería. ■

Lema 2.4.2 *Para cada $n \in \mathbb{Z}$, tenemos*

$$\frac{t^n-1}{t-1} \equiv n \bmod(t-1). \tag{2.8}$$

Prueba. Notemos que para $n>0$

$$\frac{t^n-1}{t-1}=t^{n-1}+\cdots+t+1=\left(t^{n-1}-1\right)+\cdots+\left(t-1\right)+n=\left(t-1\right)h\left(t\right)+n,$$

así (2.8) se cumple. Para $n<0$, tenemos

$$\begin{aligned}\frac{t^n-1}{t-1} &= \frac{t^n\left(1-t^{-n}\right)}{t-1}=t^n\left(t^{-n-1}+\cdots+t+1\right)=t^{-1}+t^{-2}+\cdots+t^n \\ &= \left(t^{-1}-1\right)+\left(t^{-2}-1\right)+\cdots+\left(t^n-1\right)+n \\ &= -t^{-1}\left(t-1\right)-t^2\left(t^2-1\right)-\cdots-t^n\left(t^n-1\right)+n=r\left(t,t^{-1}\right)\left(t-1\right)+n,\end{aligned}$$

luego, (2.8) también se cumple.

Finalmente el caso $n=0$ se cumple trivialmente. ■

Lema 2.4.3 *Supongamos que la característica de F es cero. Entonces para $n \in F\left[t,t^{-1}\right]$, n es un entero no nulo, si y sólo si, $n|1, n-1|1$ ó $n+1|1$, y existe una potencia x de t, tal que* $\dfrac{x-1}{t-1} \equiv n \bmod(t-1)$.

Prueba. Supongamos que n es un entero no nulo en $F\left[t,t^{-1}\right]$, entonces obviamente $n-1$ ó $n+1$ es también un entero no nulo, ya que la característica de F es cero. Así, $n|1$ y $n-1|1$ ó $n+1|1$. Además, para $x=t^n$ tenemos que $\dfrac{x-1}{t-1} \equiv n \left(\bmod t-1\right)$, por el lema 2.4.2. Recíprocamente, supongamos que $n \in F\left[t,t^{-1}\right]$ cumple dichas propiedades. Así, en virtud de que $n|1$, tenemos que $n=mt^s$, para algún $m \in F$ y $s \in \mathbb{Z}$. Supongamos que $n-1|1$(el otro caso se demuestra de manera analoga), luego $mt^s-1|1$, por lo tanto, el polinomio mt^s-1 debe

ser un monomio, lo cual implica que $s = 0$, es decir, n es una constante. Finalmente, sabemos que existe $n_0 \in \mathbb{Z} \setminus \{0\}$ tal que

$$\frac{t^{n_0} - 1}{t - 1} \equiv n \,(\mathrm{mod}\, t - 1)\,,$$

y, por el lema 2.4.2, tenemos

$$\frac{t^{n_0} - 1}{t - 1} \equiv n_0 \,(\mathrm{mod}\, t - 1)\,,$$

de este modo $n \equiv n_0 \,(\mathrm{mod}\, t - 1)$. Así, existe un polinomio $k\left(t, t^{-1}\right)$ tal que $n - n_0 = (t-1)\,k\left(t, t^{-1}\right)$. Al evaluar $t = 1$ obtenemos $n = n_0$ y por tanto $n \in \mathbb{Z} \setminus \{0\}$. ■

Lema 2.4.4 *Sobre $F\left[t, t^{-1}\right]$ los conjuntos positivo-existenciales coinciden con los conjuntos diofantinos en el lenguaje $(+, \cdot, 0, 1, t)$.*

Prueba. En virtud de la proposición 2.1.1, es suficiente encontrar polinomios f y g en $\mathbb{Z}\,[t]\,[x, y]$ que satisfagan (2.3) y (2.4), respectivamente.

Como $F\left[t, t^{-1}\right]$ es un dominio, el polinomio $g\,(x, y) = xy$ cumple (2.4). Además, el polinomio $h\,(x) = x^2 - t \in \mathbb{Z}\,[t]\,[x, y]$, no tiene raíces en el campo de fracciones de $F\left[t, t^{-1}\right]$, $F\left(t, t^{-1}\right)$. En efecto, si $x_0 = \dfrac{P\left(t, t^{-1}\right)}{Q\left(t, t^{-1}\right)}$ fuera raiz de h, entonces $P^2\left(t, t^{-1}\right) = tQ^2\left(t, t^{-1}\right)$ lo cual es absurdo ya que el grado del lado izquierdo es un entero par y el grado del lado derecho es un entero impar. De este modo, como ya habíamos visto, el polinomio $f\,(x, y) = y^2 h\left(\dfrac{x}{y}\right)$ satisface (2.3) y así, probamos nuestro lema. ■

Teorema 2.4.5 *Sea F un campo de característica cero. Entonces la teoría diofantina sobre $F\left[t, t^{-1}\right]$ en el lenguaje $(+, \cdot, 0, 1, t)$ es indecidible. O, en forma equivalente, $H10_{\mathbb{Z}[t]}\left(F\left[t, t^{-1}\right]\right)$ es insoluble.*

Prueba. Por los lemas 2.4.1 y 2.4.4, podemos expresar el hecho de que x sea una potencia de t por una fórmula existencial de la siguiente forma:

$$\pi\,(x) \equiv (\exists w, v)\,(x \neq 0 \wedge 1 = xw \wedge x - 1 = (t-1)\,v)\,,$$

de hecho $\pi\,(x)$ puede tomarse de la siguiente forma

$$\pi\,(x) \equiv (\exists w, v)\,(1 = xw \wedge x - 1 = (t-1)\,v)\,,$$

donde, en virtud del lema 2.4.4, $\pi\,(x)$ puede suponerse como una fórmula diofantina sobre $F\left[t, t^{-1}\right]$. Por el lema 2.4.3, el hecho de que un número n en $F\left[t, t^{-1}\right]$ sea entero puede

expresarse por medio de la siguiente fórmula:

$$\begin{aligned}\psi(n) &\equiv (\exists x,y,z,w)\,(n=0\vee(\pi(x)\wedge x+1=(t-1)\,n+y\,(n-1)^2\\ \wedge nz &= 1\wedge((n+1)\,w=1\vee(n-1)\,w=1)),\end{aligned}$$

de nuevo, en virtud del lema 1.29, $\psi(n)$ puede tomarse como una fórmula diofantina. Supongamos, por contradicción, que $H10_{\mathbb{Z}[t]}\left(F\left[t,t^{-1}\right]\right)$ es soluble. Entonces, para una ecuación diofantina $P(x_1,\ldots,x_n)=0$ tendríamos que

$$(\exists x_1,\ldots,x_n\in\mathbb{Z})\left[P(x_1,\ldots,x_n)=0\right],$$

si y sólo si,

$$\left(\exists x_1,\ldots,x_n\in F\left[t,t^{-1}\right]\right)\left(P(x_1,\ldots,x_n)=0\wedge\psi(x_1)\wedge\ldots\wedge\psi(x_n)\right). \tag{2.9}$$

Pero la sentencia (2.9) puede tomarse diofantina y de este modo podríamos decidir $H10(\mathbb{Z})$, lo cual es absurdo. ■

2.5 La teoría diofantina sobre anillos cuadráticos reales

Una anillo cuadrático real $A(D)$ es el anillo de enteros del campo $\mathbb{Q}\left(\sqrt{D}\right)$, es decir, el conjunto de elementos de $\mathbb{Q}\left(\sqrt{D}\right)$ que satisfacen un polinomio mónico con coeficientes en $\mathbb{Z}$. Además, $D>1$ es un número natural libre de cuadrados, lo que significa que ningún cuadrado perfecto, no trivial, lo divide, o en forma equivalente D tiene la forma $D=P_1.P_2\ldots P_n$, donde los P_i son primos distintos. La razón por la cual se consideran números libres de cuadrados y no simplemente números naturales que no son cuadrados es el siguiente hecho elemental: todo número natural se puede expresar de manera única como el producto de un cuadrado perfecto y un número libre de cuadrados. Es decir, si $D=a^2D_1$, con D_1 libre de cuadrados, entonces la información aritmética interesante del anillo $A(D)$ la contiene el anillo $A(D_1)$, ya que $\sqrt{D}$ es simplemente un múltiplo entero de $\sqrt{D_1}$. Recordemos que si $\alpha=a+b\sqrt{D}$ entonces la norma de α se define como $N(\alpha)=\alpha\overline{\alpha}$, donde $\overline{\alpha}=a-b\sqrt{D}$ denota el conjugado de α. Es obvio que $A(D)\subseteq\mathbb{R}$; así, los polinomios $f(x,y)=x^2+y^2$ y $g(x,y)=xy$ satisfacen las hipótesis de la proposición 2.1.1 y tenemos que la colección de los conjuntos positivo-existenciales coincide con la colección de los conjuntos diofantinos sobre $A(D)$. En esta sección mostraremos que $H10(A(D))$ es insoluble o, lo que es equivalente, que la teoría positivo-existencial sobre $A(D)$ es indecidible. Para esto, mostraremos que $\mathbb{N}$ es un subconjunto diofantino de $A(D)$, y de este modo la insolubilidad de $H10(\mathbb{N})$ implicará automáticamente la de $H10(A(D))$.

Similarmente haremos uso de la ecuación de Pell y de nuevo supondremos soluciones no

triviales para $x^2 - Fy^2 = 1$, donde F es un número natural que no es un cuadrado perfecto.

A continuación probaremos un último lema sobre la ecuación de Pell. Para recordar la notación se sugiere al lector ver la Sección 3 del Capítulo 1.

Lema 2.5.1 *Sean $A, n, j \in \mathbb{N}$, con $A > 1$. Entonces*

$$Y_A(nj)^2 \equiv Y_A(n)^2 j^2 \left(\mathrm{mod}\, Y_A(n)^4\right).$$

Prueba. En virtud de (1.33) tenemos que

$$\frac{Y_A(nj)}{Y_A(n)} \equiv jX_A(n)^{j-1} \left(\mathrm{mod}\, Y_A(n)^2\right).$$

Elevando al cuadrado obtenemos

$$\frac{Y_A(nj)^2}{Y_A(n)^2} \equiv j^2 X_A(n)^{2j-2} \left(\mathrm{mod}\, Y_A(n)^2\right).$$

Ahora, $X_A(n) \equiv 1 \,\mathrm{mod}(Y_A(n)^2)$, lo cual implica que

$$\frac{Y_A(nj)^2}{Y_A(n)^2} \equiv j^2 \left(\mathrm{mod}\, Y_A(n)^2\right)$$

de donde se concluye inmediatamente el lema. ■

Lema 2.5.2 *Sea $A(D)$ un anillo cuadrático real. Sea (A, B) una solución no trivial $(B \neq 0)$ de la ecuación de Pell $A^2 - DB^2 = 1$ y $E = A^2 - 1$. Si para $x, y \in A(D)$ se cumple $x^2 - Ey^2 = 1$, entonces $y^2 \in \mathbb{N}$.*

Prueba. Obviamente $A > 1$ y $E = B^2 D$. Adicionalmente,

$$\left(x - B\sqrt{D}y\right)\left(x + B\sqrt{D}y\right) = 1.$$

Por lo tanto, $x+B\sqrt{D}y$ es una unidad en $A(D)$. Sea $v = x+B\sqrt{D}y$, luego $v^{-1} = \overline{v} = x-B\sqrt{D}y$. Ahora,

$$v^2 - 2vv^{-1} + \left(v^{-1}\right)^2 = \left(v - \left(v^{-1}\right)^2\right) = \left(2B\sqrt{D}y\right)^2 = 4B^2Dy^2,$$

y en consecuencia $4B^2Dy^2 + 2 = v^2 + \overline{v}^2$. Pero para cada $h \in A(D)$, se cumple que $h + \overline{h} \in \mathbb{Q} \cap A(D)$. Por lo tanto, $4B^2Dy^2 + 2 \in \mathbb{Q}$ y de este modo $y^2 \in \mathbb{Q}$. Finalmente, dado que los únicos números racionales que pertenecen a $A(D)$ son los números enteros (si $\alpha \in \mathbb{Q}$ satisface un polinomio mónico en $\mathbb{Z}[t]$, entonces $\alpha \in \mathbb{Z}$) y $y^2 \in A(D)$, concluimos que $y^2 \in \mathbb{Z}$. Más aún, $y^2 \in \mathbb{N}$. ■

Lema 2.5.3 *Sea* $D > 1, x, y, z \in A(D)$. *Si* $x \equiv y \pmod{z}$ *con* $0 \leq x < z, 0 \leq \overline{x} < \overline{z}, 0 \leq y < z, 0 \leq \overline{y} < \overline{z}$ *entonces* $x = y$.

Prueba. Supongamos que $x \neq y$, entonces $x - y = zw$, con $w \neq 0$. Así que

$$|x - y|\,|\overline{x} - \overline{y}| = |z\overline{z}|\,|N(w)|.$$

Pero $|N(w)| \geq 1$, y de este modo

$$|x - y|\,|\overline{x} - \overline{y}| \geq |z\overline{z}|,$$

lo cual es absurdo, ya que por hipótesis se tiene que

$$|x - y|\,|\overline{x} - \overline{y}| \leq (\max\{x, , y\}).(\max\{\overline{x}, \overline{y}\}) < z\overline{z} = |z\overline{z}|.$$

■

Lema 2.5.4 *Sea* $A(D)$ *un anillo cuadrático real y sea* E *como en la hipótesis del lema 2.5.2. Denotemos por* π *al siguiente sistema de ecuaciones diofantinas en las variables* $x, y, u, v, z, w, h, q, r, s$.

$$x^2 - Ey^2 = 1 \tag{2.10}$$

$$u^2 - Ev^2 = 1 \tag{2.11}$$

$$v^2 - y^2 t = zy^4 \tag{2.12}$$

$$t = w^2 \tag{2.13}$$

$$y^2 - t = 1 + h^2 + q^2 + r^2 + s^2 \tag{2.14}$$

Entonces:

a) Si el sistema π *tiene una solución* $(t, x, \ldots, s)$ *en* $A(D)$ *se cumple que* $t \in \mathbb{Z}$.

b) Si $k \in \mathbb{N}, k \neq 0$, *el sistema* π *tiene una solución* $(t, x, \ldots, s)$ *con* $t = n^2$.

Prueba. *a*) Supongamos que $(t, x, \ldots, s)$ es una solución de π. De (2.10) y (2.11) y el lema 2.5.2 se sigue que $y^2 \in \mathbb{N}, v^2 \in \mathbb{N}$. Notemos que $y \neq 0$, ya que si $y = 0$, de (2.13) se seguiría que $t \geq 0$ y de (2.14) que $t < 0$, lo cual es absurdo. Ahora, de (2.12) concluimos que $\dfrac{v^2}{y^2} \equiv t \pmod{y^2}$. Tomando conjugados $\dfrac{v^2}{y^2} \equiv \overline{t} \pmod{y^2}$, luego $t \equiv \overline{t} \pmod{y^2}$, por (2.13) y (2.14) $0 \leq t \leq y^2$. Finalmente, usando el lema 2.5.3, $\overline{t} = t$; por lo tanto $t \in \mathbb{Q} \cap A(D) = \mathbb{Z}$.

b) Supongamos que $t = k^2$, con $k \in \mathbb{N}$. Sabemos que $E = A^2 - 1$, sea $n \in \mathbb{N}$ tal que

$Y_A(n) > k$. Definamos

$$x = X_A(n),\ y = Y_A(n),\ u = x = X_A(nk),\ v = Y_A(nk),\ w = k.$$

Claramente, (2.10) y (2.11) se cumplen. Por el lema 2.5.1 podemos escoger z tal que (2.12) se cumpla. Obviamente (2.13) se satisface. Finalmente, $y^2 - k^2 > 0$, o sea, $y^2 - k^2 - 1 \geq 0$, y por el teorema de Lagrange podemos satisfacer (2.14). ■

Teorema 2.5.5 *El décimo problema de Hilbert sobre $A(D)$ es insoluble.*

Prueba. Denotemos por $\psi(t_i)$ a la siguiente sentencia diofantina con única variable libre t_i

$$(\exists x, y, z, u, v, w, h, q, r, s)(\pi(t_i)),$$

donde $\pi(t_i)$ denota el sistema π reemplazando t por t_i. Entonces, en virtud del lema 2.5.3 y del teorema de Lagrange, para $n \in A(D)$, n es un número natural, si y sólo si,

$$(\exists t_1, t_2, t_3, t_4)\left(\pi(t_1) \wedge \pi(t_2) \wedge \pi(t_3) \wedge \pi(t_4) \wedge n = t_1^2 + t_2^2 + t_3^2 + t_4^2\right).$$

Así, el conjunto de los números naturales de diofanitno en $A(D)$, luego si $H10(A(D))$ fuera decidible, $H10(\mathbb{N})$ lo sería, lo cual es absurdo. De donde concluimos nuestro teorema. ■

Capítulo 3

EL DÉCIMO PROBLEMA DE HILBERT PARA LOS NÚMEROS RACIONALES

3.1 ¿Qué se conoce?

En este capítulo pretendemos mostrar, a manera de información, y sin dar demostraciones, las conjeturas y resultados más importantes conocidos hasta la fecha sobre el problema $H10\,(\mathbb{Q})$.

El problema de determinar si una ecuación difonatina tiene soluciones en los racionales se remonta al mismo Diofanto, que no sólo resolvió ecuaciones en los naturales o en los enteros, sino que también buscó resolverlas en $\mathbb{Q}$. El análisis diofantino se desarrolló del mismo modo hasta 1900, y por eso resulta curioso que Hilbert no se preguntara por un "método" para resolver ecuaciones diofantinas sobre números racionales. Es posible que Hilbert fuera optimista y pensara que existía un algoritmo para resolver ecuaciones en los números enteros y dicho algoritmo también permitiría resolver ecuaciones sobre los números racionales. En efecto, resolver una ecuación diofantina $D\,(\alpha_1,\ldots,\alpha_m)=0$ en números racionales $\alpha_1,\ldots,\alpha_m$, es equivalente a resolver la ecuación

$$(z+1)^d\,D\left(\frac{x_1-y_1}{z+1},\ldots,\frac{x_m-y_m}{z+1}\right)=0,$$

en los números naturales $z,x_1,\ldots,x_m,y_1,\ldots,y_m$ (d el grado de D). Así, en virtud de que $H10\,(\mathbb{N})$ y $H10\,(\mathbb{Z})$ son equivalentes, como problemas de decisión, obtendríamos un "método" para decidir $H10\,(\mathbb{Q})$. De este modo, y de manera implícita, Hilbert preguntó en su décimo problema por un algoritmo de decisión en los números racionales. Sin embargo, como vimos en el Capítulo 1, tal algoritmo de decisión para $\mathbb{N}$ no existe. Este hecho parece no tener implicaciones directas sobre la decibilidad o indecibilidad de $H10\,(\mathbb{Q})$. Más aún, como veremos más adelante $H10\,(\mathbb{Q})$ es equivalente al décimo problema de Hilbert sobre la clase de todas las *ecuaciones diofantinas homogéneas*. Éstas forman una subclase muy particular de las ecuaciones diofantinas y podría existir un algoritmo para decidir sobre ellas.

De otro lado, aunque $H10\,(\mathbb{Z})$ es insoluble, es natural preguntarse para qué clases de ecuaciones es posible encontrar un algoritmo de decisión. Pensemos por un momento en soluciones enteras; claramente, si $f\,(x_1,\ldots,x_n)=0$ tiene soluciones en $\mathbb{Z}^n$, las tiene en $\mathbb{R}^n$ y para cada entero $M>1$ las congruencias $f\,(x_1,\ldots,x_n)\equiv 0\,(\mathrm{mod}\,M)$ tienen solución. Por el Teorema Chino del Residuo las congruencias módulo M se reducen a congruencias módulo p^n para cada primo

p y cada $n \geq 1$. Lo anterior proporciona un criterio útil para mostrar que ciertas ecuaciones no tienen soluciones enteras. Por ejemplo, la curva elíptica

$$y^2 = z^3 + 7, \tag{3.1}$$

no tiene soluciones en $\mathbb{Z}$ (pero sí en $\mathbb{R}$) ya que si $(x, y) \in \mathbb{Z}^2$ es una solución de 3.1, entonces x no puede ser par debido a que la congruencia

$$y^2 \equiv 7 \pmod 8$$

no tiene solución (verificacion finitista). Además,

$$y^2 + 1 = x^3 + 8 = (x + 2)\left(x^2 - 2x + 4\right)$$

y como $x - 1$ es par

$$x^2 - 2x + 8 = (x - 1)^2 + 3 \equiv 3 \pmod 4.$$

Ahora, como producto de números de la forma $4n + 1$ sigue siendo de esta forma, concluimos que $x^2 - 2x + 8$ tiene un factor primo p, con $p \equiv 3 \pmod 4$. Por lo tanto, la congruencia $y^2 \equiv -1 \pmod p$ tiene solución, lo cual es un absurdo, ya que -1 sólo es residuo cuadrático para primos congruentes con uno módulo cuatro (esta solución es de V. Lebesgue). No obstante, la condición de solubilidad real y las congruencias módulo p^n no son suficientes para garantizar soluciones enteras, ya que por ejemplo, la ecuación

$$(2x + 3)(5x + 7) = 0 \tag{3.2}$$

tiene soluciones reales y módulo p^n, para cada primo p y $n \geq 1$, pero obviamente no las tiene en $\mathbb{Z}$. La razón por la cual 3.2 tiene soluciones en congruencias es básicamente que para cada primo p y $n \geq 1$, el número p^n es primo relativo con 2 ó 5, y de este modo, cualquier número natural se puede expresar como combinación lineal de p^n y 2 ó 5, por lo cual existe un x que anula a alguno de los 2 factores de (3.2) (dependiendo del primo p que se escoja). Conviene mencionar, en este punto, que resolver ecuaciones diofantinas en $\mathbb{R}$ es algorítmicamente soluble [27]. Para cada p y n fijos, decidir si $f(x_1, \ldots, x_n) \equiv 0 \pmod{p^n}$ es en el peor de los casos una verificación finita. En 1963, Nerode [15] demostró que si fijamos un primo p arbitrario, entonces existe un algoritmo que para cada ecuación diofantina $f(x_1, \ldots, x_n) = 0$, decide si las infinitas congruencias

$$f(x_{i,1}, \ldots, x_{i,n}) \equiv 0 \left(\mathrm{mod}\, p^i\right), i = 1, 2, \ldots$$

tienen o no soluciones. Este fue un buen avance pero quedaban infinitos primos que verificar. Sorprendentemente, en 1967 Ax [1] demostró que existe un algoritmo que para cada ecuación,

decide si hay solución a la congruencia módulo p^n, para cada primo p y cada $n \geq 1$. La ecuación 3.2 tiene, de manera obvia, soluciones racionales. Se podría intuir que las condiciones de solubilidad real y de las congruencias, si bien no implican una solución entera podrían implicar una solución racional. Infortunadamente, esto no es verdad ya que la ecuación

$$h(x) = \left(x^2 - 13\right)\left(x^2 - 17\right)\left(x^2 - 221\right) = 0$$

tiene soluciones en $\mathbb{R}$ y módulo p^n, para cada primo p y cada $n \geq 1$, pero claramente no tiene soluciones racionales. A continuación, bosquejaremos la razón por la cual lo anterior es cierto. Primero, para un primo fijo p, la propiedad multiplicativa del símbolo de Legrende

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right),$$

(recordemos que si $(a,p) = 1$, entonces $\left(\frac{a}{p}\right)$ se define como 1 si a es un residuo cuadrático módulo p y -1 si a no lo es), muestra que si 13 y 17 no son residuos cuadráticos módulo p, entonces $17 \times 13 = 221$ lo es. Ádemas, trivialmente se verifica que $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right)$. Así, algunas de las siguientes congruencias tiene solución:

$$\begin{aligned} x^2 - 13 &\equiv 0 \pmod{p}, \\ x^2 - 17 &\equiv 0 \pmod{p}, \\ x^2 - 221 &\equiv 0 \pmod{p}. \end{aligned}$$

Al fijar una solución a de alguna de las congruencias anteriores y haciendo todas las cuentas, es posible mostrar que

$$h'(a) \not\equiv \pmod{p},$$

y de este modo, usando la siguiente versión del *lema de Hensel*, obtenemos el resultado:

Si $t \in \mathbb{Z}[x]$ y $a \in \mathbb{Z}$ satisface $f(a) \equiv 0 \pmod{p}$ y $f'(a) \not\equiv 0 \pmod{p}$, entonces para cada $n \geq 1$ la congruencia $f(x) \equiv 0 \pmod{p^n}$ tiene una solución a_n.

En conclusión, por los teoremas de Ax y Tarski, el conjunto de todas las ecuaciones diofantinas que tienen solución real y soluciones módulo M $(M > 1)$ es recursivo. Y el conjunto de ecuaciones con soluciones enteras es un subconjunto propio de éste. De este modo, aunque no exista un algoritmo de decisión en los enteros, el algoritmo de Ax-Tarski nos proporciona información importante en muchos casos sobre la solubilidad de una ecuación en $\mathbb{Z}$ o en $\mathbb{Q}$.

Volviendo a $H10(\mathbb{Q})$, a continuación mostraremos una equivalencia interesante de este problema, pero antes recordemos que una ecuación diofantina $f(x_1, \ldots, x_n) = 0$ es *homogénea de grado m*, si todos los monomios que forman a f son de grado m, o equivalentemente si para

cada $\lambda \in \mathbb{R}$, se cumple

$$f(\lambda x_1, \ldots, \lambda x_n) = \lambda^m f(x_1, \ldots, x_n). \tag{3.3}$$

A f se le conoce como una forma de grado m. Claramente, una ecuación homogénea tiene la solución trivial $(0, 0, \ldots, 0)$. Llamaremos a una solución $(x_1, \ldots, x_n)$ no trivial, si algún $x_i \neq 0$. Además, de (3.3) es claro que una ecuación homogénea tiene soluciones enteras no triviales, si y sólo si, tiene soluciones racionales no triviales.

Teorema 3.1.1 *$H10(\mathbb{Q})$ es equivalente a decidir si ecuaciones diofantinas homogéneas tienen o no soluciones no triviales.*

Prueba. Primero reduzcamos $H10(\mathbb{Q})$ al problema sobre formas. Sea $P(x_1, \ldots, x_n) = 0$ una ecuación diofantina para la cual deseamos saber si tiene soluciones en $\mathbb{Q}^n$.

Sea $R(x_1, \ldots, x_n, u) = u^d P\left(\frac{x_1}{u}, \ldots, \frac{x_n}{u}\right)$ la homogenización de P, donde n es el grado de P. Definamos

$$\begin{aligned} S(x_1, \ldots, x_n, r_1, \ldots, r_4, y) &= \sum_{i=1}^{n} x_i^2 + \sum_{i=1}^{4} r^2 - y^2, \\ T(y, z, u) &= y^2 - 2z^2 - u^2. \end{aligned}$$

Notemos que $P = 0$ tiene soluciones en $\mathbb{Q}^n$, si y sólo si, $R = 0$ tiene soluciones en $\mathbb{Z}^{n+1}$ con $u \neq 0$. Sea

$$D = R^4 + S^{2d} + T^{2d},$$

luego, D es una forma de grado $4d$ en $n + 7$ variables con coeficientes en $\mathbb{Z}$.

De otro lado, por los resultados obtenidos en la Sección 3 del Capítulo 1, sabemos que la ecuación de Pell

$$x^2 - 2y^2 = 1, \tag{3.4}$$

tiene infinitas soluciones, ya que (3.4) tiene solución no trivial $(3, 2)$. De donde concluimos que (3.4) tiene soluciones con x arbitrariamente grande.

Así, para cualquier número natural $a > 0$, al multiplicar ambos lados de (3.4) por a^2 tenemos que la ecuación $x^2 - 2y^2 = a^2$ tiene soluciones con x arbitrariamente grande.

Veamos que $P = 0$ tiene soluciones en $\mathbb{Q}$, si y sólo si, $D = 0$ tiene solución no trivial en $\mathbb{Z}^{n+7}$ (o $\mathbb{Q}^{n+7}$). Supongamos que $P = 0$ tiene soluciones en $\mathbb{Q}^n$, entonces $R(x_1, \ldots, x_n, u) = 0$ tiene soluciones con $u \neq 0$. Ahora, por lo anterior, $y^2 - az^2 = u^2$ tiene soluciones con $y^2 > \sum_{i=1}^{n} x_i^2$, y por el teorema de Lagrange, existen $r_1, \ldots, r_4 \in \mathbb{Z}$, tales que

$$\sum_{i=1}^{n} x_i^2 - y^2 + \sum_{i=1}^{n} r_i^2 = 0.$$

Así, $R = 0, T = 0$ y $S = 0$, por lo tanto, la ecuación $D = 0$ tiene una solución no trivial ($y \neq 0$). En la otra dirección, supongamos que

$$D(x_1, \ldots, x_n, r_1, \ldots, r_4, u, y, z) = 0$$

tiene solución con alguna variable no nula. Si $y = 0$, dado que $T = S = 0$, tenemos que $z = u = 0$,

$$r_1 = \cdots = r_4 = x_1 = \cdots = x_n = 0,$$

lo cual es absurdo. Como $y \neq 0$ y $\sqrt{2} \notin \mathbb{Q}$, entonces $u \neq 0$. Así, $R = 0$ y $u \neq 0$, por lo tanto $P = 0$, tiene soluciones en $\mathbb{Q}^n$.

Recíprocamente, sea $f(x_1, \ldots, x_n) = 0$ una ecuación diofantina homogénea. Entonces, es fácil verificar, utilizando (3.3), que nuestra ecuación tiene soluciones no triviales en $\mathbb{Z}$ si y sólo si la ecuación

$$f(1, \ldots, x_n) f(x_1, 1, \ldots, x_n) \cdots f(x_1, \ldots, 1) = 0,$$

tiene soluciones en $\mathbb{Q}^n$. ■

El teorema anterior está motivado por el hecho empírico de que hay más métodos para decidir solubilidad (no trivial) de formas que para decidir solubilidad de polinomios no homogéneos. Precisando un poco, en el mundo de los polinomios homogéneo existe un fenómeno muy interesante: formas con muchas variables respecto a su grado tiene automáticamente soluciones no triviales en $\mathbb{Q}$. Por ejemplo, Meyer en 1884 demostró que una forma diofantina cuadrática en por lo menos cinco variables tiene una solución no trivial en $\mathbb{Z}$, si es indefinida, es decir, si tiene una solución no trivial en $\mathbb{R}$. De hecho para formas cuadraticas vale el famoso *teorema de Hasse-Minkowski,* el cual afirma que una forma cuadrática tiene soluciones no triviales en $\mathbb{Q}$ si y sólo si tiene soluciones no triviales en $\mathbb{R}$ y módulo M, para cada $M > 1$. En particular, esto implica que podemos decidir solubilidad de formas cuadráticas. El caso de formas cúbicas está abierto y la matemática que ha generado es increible. Quizá el resultado más interesante y "hermoso" es el obtenido por Davenport hace más de 40 años, el cual afirma que toda forma diofantina cúbica tiene soluciones no triviales en $\mathbb{Q}$ si tiene más de 15 variables. Otro resultado también interesante es el de Birch: si $d \geq 1$ es un entero impar, entonces existe un número $n(d)$ tal que para toda forma F de grado d en n variables, con $n > n(d)$, la ecuación $F = 0$ tiene soluciones no triviales en $\mathbb{Q}$. A propósito, hasta ahora no existe un algoritmo que decida, dada una curva elíptica sobre $\mathbb{Q}$, si $E(\mathbb{Q}) \neq \{\infty\}$, es decir, si la curva tiene soluciones racionales genuinas. Todo lo anterior nos muestra que hay grandes familias de ecuaciones que tiene soluciones racionales, claramente no hay problema para decidir sobre estas ecuaciones. Así, podría ser plausible pensar que $H10(\mathbb{Q})$ es soluble.

Cambiando completamente de perspectiva, es bastante natural preguntarse si $\mathbb{Z}$ es diofantino

en $\mathbb{Q}$, es decir, si existe un polinomio diofantino $P(x_1, \ldots, x_m)$ tal que

$$x \in \mathbb{Z} \Leftrightarrow (\exists x_1, \ldots, x_m \in \mathbb{Q})\,[P(x, x_1, \ldots, x_m) = 0]\,,$$

lo cual implicaría, que $H10(\mathbb{Q})$ es insoluble, ya que de existir un algoritmo para decidir $H10(\mathbb{Q})$ este algortimo decidiría también $H10(\mathbb{Z})$. En efecto, sea $R(x_1, \ldots, x_n) = 0$ una ecuación diofantina. Entonces $R = 0$ tiene soluciones enteras si y sólo si

$$(\exists y_1, \ldots, y_n, x_{1,1}, \ldots, x_{1,m}, \ldots, x_{n,m} \in \mathbb{Q})\,(R(y_1, \ldots, y_n) = 0 \wedge P(y_1, x_{1,1}, \ldots, x_{1,m}) = 0$$

$$\wedge P(y_1, x_{1,1}, \ldots, x_{1,m}) = 0 \wedge \cdots \wedge P(y_n, x_{n,1}, \ldots, x_{n,m}) = 0).$$

Así, usando el hecho de que los conjuntos existenciales y diofantinos sobre $\mathbb{Q}$ son los mismos $(\mathbb{Q} \subseteq \mathbb{R})$, podríamos reducir $H10(\mathbb{Z})$ a $H10(\mathbb{Q})$, luego el último problema tendría que ser insoluble ya que el primero lo es.

Mostrar la diofantinidad de $\mathbb{Z}$ en $\mathbb{Q}$ podría parecer a primera vista mucho más sencillo que fabricar un método para decidir $H10(\mathbb{Q})$. Sin embargo, este es un problema abierto y no hay una idea muy clara si éste pueda ser cierto. Un primer intento por aclarar el asunto fue el de eliminar denominadores de un número racional r de manera diofantina. A continuación veremos como Julia y Rafael Robinson usaron un teorema de Gauss para eliminar el primo 2.

En su famos libro "Disquisiciones Aritmeticae", Gauss probó el siguiente bello teorema, el cual caracteriza los números naturales que se pueden escribir como la suma de tres cuadrados.

Teorema 3.1.2 *Sea $m \geq 1, m = 4^n u, 4 \nmid u$. Entonces, m es la suma de tres cuadrados si y sólo si $u \not\equiv 7 \pmod 8$.*

Usando este teorema mostraremos el lema principal de Julia y Rafael Robinson.

Lema 3.1.3 *Sea $m \in \mathbb{Z}$. Entonces existen $p, q, r \in \mathbb{Q}$ tales que $p^2 + q^2 + r^2 = m$ si y sólo si existen $x, y, z \in \mathbb{Z}$ tales que $x^2 + y^2 + z^2 = m$.*

Prueba. Supongamos que $p = \dfrac{a}{b}, q = \dfrac{c}{d}, r = \dfrac{e}{f}$, satisfacen $p^2 + q^2 + r^2 = m$, luego

$$(adf)^2 + (cbf)^2 + (ebd)^2 = m\,(dbf)^2\,. \tag{3.5}$$

Hagamos $m = 4^n u$, con $4 \nmid u$. Luego, en virtud del teorema de Gauss tenemos que mostrar que $u \not\equiv 7 \pmod 8$. Sea $bdf = 4^r v$, con $4 \nmid v$. De esta manera, $m\,(bdf)^2 = 4^{n+2r} uv$. Ahora, aplicamos el teorema de Gauss a este número para concluir $u \not\equiv 7 \pmod 8$. Esto lo haremos investigando la paridad de v.

Supongamos que $4 \nmid uv^2$, luego por (3.5) se tiene que $uv^2 \not\equiv 7 \pmod 8$. Por otro lado, $v \equiv 1, 3, 5, 7 \pmod 8$ y así, elevando al cuadrado cada uno de estos valores vemos que $v^2 \equiv$

$1 \pmod 8$, y por lo tanto, $u \not\equiv 7 \pmod 8$. Supongamos que $v \equiv 0 \pmod 2$, pero $4 \nmid v$. Entonces, $v = 2s$, con $s \equiv 1 \pmod 2$, así $m(bdf)^2 = 4^{n+2r+1}us^2$, con $4 \nmid us^2$. Ahora, como s es impar $s^2 \equiv 1 \pmod 8$. Como en el caso anterior $us^2 \not\equiv 7 \pmod 8$ y de este modo $u \not\equiv 7 \pmod 8$. Esto termina la demostración. ■

Sea $R = \left\{ \frac{n}{m} \mid (m,n) = 1, (m,2) = 1 \right\}$. Entonces R es un subanillo de $\mathbb{Q}$, el subanillo de todas las fracciones con denominador impar.

Teorema 3.1.4 *R es un subconjunto diofantino de $\mathbb{Q}$. Precisando, para $x \in \mathbb{Q}$ vale lo siguiente:*

$$x \in R \Leftrightarrow (\exists a, b, c \in \mathbb{Q}) \left(7x^2 + 2 = a^2 + b^2 + c^2\right).$$

Prueba. Supongamos que existen $x, a, b, c \in \mathbb{Q}$ tales que $7x^2 + 2 = a^2 + b^2 + c^2$, y que $x = \frac{n}{2^t m}$ con $(n,m) = 1, 2 \nmid n$ y $t \geq 1$. Eliminando denominadores del lado izquierdo vemos que $7n^2 + 2.2^{2t}m^2$ es la suma de tres cuadrados en $\mathbb{Q}$. Por el lema 3.1.3, podemos tomar los cuadrados en $\mathbb{Z}$. Como n es impar tenemos que $7n^2 + 2.2^{2t}m^2 \equiv 7n^2 \equiv 7 \pmod 8$. De esto concluimos que $7n^2 + 2.2^{2t}m^2 = 7 + 8k$, para algún $k \in \mathbb{Z}$. Ahora, los números de la forma $7 + 8k$ son de la forma $4^0 u$, $4 \not| u$, por lo tanto, $u \equiv 7 \pmod 8$, lo cual contradice el teorema 3.1.2.

Recíprocamente, sea $x = \frac{n}{m}$, con $(m,n) = (2,m) = 1$. Entonces $7x^2 + 2$ es la suma de tres cuadrados si y sólo si $7n^2 + 2m^2$ es la suma de tres cuadrados si y sólo si $7n^2 + 2m^2$ no es de la forma $4^s(8k + 7)$. Probaremos lo último por contradicción. Supongamos primero que $s \geq 1$. Tenemos entonces que $2|7n^2$, así $4|7n^2$. Como $4|(7n^2 + 2m^2)$ tenemos que $4|2m^2$, de aquí m es par, lo cual es absurdo. Si $s = 0$, entonces $7n^2 + 2m^2 = 7 + 8k$, así $7n^2 + 2m^2 \equiv 7 \pmod 8$. Como m es impar se sigue que $7n^2 + 2 \equiv 7 \pmod 8$, lo cual no se cumple para ningún valor de n. De este modo, $7n^2 + 2m^2$ no es de la forma $4^s(8k + 7)$ lo cual termina la demostración. ■

Aunque la demostración del teorema 3.1.4 sólo usa hechos de la teoría elemental de números, la quisimos exponer completamente para destacar la falta de métodos generales y potentes para atacar problemas como el de la diofantinidad de $\mathbb{Z}$ en $\mathbb{Q}$. En general, se han usado métodos ad hoc y trucos para resolver casos particulares de este problema. A propósito, Julia Robinson, en 1949, encontró como eliminar cada primo del denominador. Luego, usando el hecho de que la intersección de conjuntos diofantinos sobre $\mathbb{Q}$ es diofantina tenemos lo siguiente:

$$R_S = \left\{ \frac{m}{n} \mid (m,n) = 1, (s,n) = 1, \text{ para cada } s \in S \right\}$$

es diofantino en $\mathbb{Q}$, para cada conjunto finito de primos S. Todavia estamos "infinitamente lejos" de $\mathbb{Z}$. Sólo en 2002, Poonen logró mejorar sorprendentemente estos resultados. Más adelante, hablaremos un poco de su teorema.

Otro hecho empírico que hace plausible de la veracidad de la conjetura ($\mathbb{Z}$ diofantino en $\mathbb{Q}$) es el hecho de que $H10_{\mathbb{Z}[t]}(F(t))$ es insoluble ($F(t)$ es el campo de fracciones $F[t]$) para

$F = \mathbb{R}$, F un campo finito, entre otros. Lo anterior se basa en que $\mathbb{Q}$ y $F(t)$ tienen bastantes propiedades comunes, aritmeticamente hablando. Además, ciertas similitudes entre $\mathbb{Q}$ y estos anillos junto con la manera en la que prueban la indecidibilidad de $H10_{\mathbb{Z}[t]}(F(t))$, probando que $\mathbb{Z}$ es diofantino en $F(t)$, brindan evidencia a favor de la conjetura. El investigador principal en esta corriente es Thanases Pheidas. De otro lado, un número no despreciable de matemáticos, que trabajan en teoría de números, están en desacuerdo con el punto de vista anterior y por lo tanto con la veracidad de esta conjetura. Bosquejaremos, a grandes rasgos, sus razones: en primer lugar, la conjetura de Mordell (Teorema de Faltings: una curva de genus ≥ 2 tiene finitos puntos racionales) nos brinda algunos recursos para decidir de manera efectiva cuestiones cualitativas acerca de los puntos racionales de la curva, precisando un poco, nos permite decidir si una curva tiene infinitos puntos racionales si miramos la curva sobre ciertas extensiones finitas de $\mathbb{Q}$ (campos de número). Además, algunas conjeturas de S. Lang permiten dar una especie de caracterización de las variedades totalmente irreducibles que tienen infinitos puntos sobre los racionales en un campo de número. Informalmente, la idea de esta conjeturas y resultados es asociar la (in)finitud de las soluciones racionales de una curva con las propieades geométricas de la variedad. Así, en este orden de ideas, es probable que el conocimiento de la geometría de variedades sobre los números racionales, nos permita efectivamente decidir cuestiones sobre los racionales. En este punto, es útil mencionar que la geometría de los números enteros es mucho más complicada que la geometría de los números racionales viéndolo desde el punto de vista de las varieadades abelianas, las cuales son una generalización de las curvas elípticas en altas dimensiones. El fenómeno más importante es que sobre variedades abelianas la geometría de los puntos racionales tienen una estructura muy manejable mientras que la geometría de los puntos enteros es prácticamente intratable. Inclusive, un buen número de lógicos (generalmente, los "pesimistas" en estas cuestiones) afirman que si la teoría diofantina sobre $\mathbb{Q}$ es indecidible será por razones "marginales" dejando la gran parte de la teoría en el terreno de lo decidible. El autor emplea un número considerable de líneas en estos comentarios para mostrarle al lector interesado que un cambio de enfoque en el problema $H10(\mathbb{Q})$ genera sorprendentes intuiciones geométricas, sobre la posible solubilidad de $H10(\mathbb{Q})$, que no se tenían al enunciar el problema.

Ahora, enunciaremos el ataque más directo a nuestra conjetura ($\mathbb{Z}$ diofantino en $\mathbb{Q}$), propuesto por B. Mazur en 1990.

Conjetura 3.1.5 *Sea $V \subseteq \mathbb{R}^n$, un conjunto algebraico diofantino definido por ecuaciones polinomiales con coeficientes en $\mathbb{Q}$. Entonces $\overline{V(\mathbb{Q})}$ tiene un número finito de componentes conexas ($\mathbb{R}^n$ con la topología usual).*

Primero notemos que $V(\mathbb{R})$ tiene un número finito de componentes conexas, éste es un hecho conocido y su demostración se puede consultar en cualquier libro de geometría algebraica real. Ahora, para variedades como $V_1 : y - x^2 = 0$ y $V_2 : y^2 - x^3 = 0$ se cumple trivialemente la

conjetura, ya que $\overline{V_i(\mathbb{Q})} = V_i(\mathbb{R})$, para $i = 1, 2$. Para la variedad $V : x^4 + y^4 - 1 = 0$ Fermat demostró que $V(\mathbb{Q}) = \{(0, \pm 1), (\pm 1, 0)\}$ y así, $\overline{V(\mathbb{Q})}$ tiene cuatro componentes conexas. Por último para la curva elíptica $C : y^2 - x^3 + 4 = 0, V(\mathbb{R})$ tiene una sola componente conexa y por el lema 2.3.1, $\overline{V(\mathbb{Q})} = V(\mathbb{R})$, así $\overline{V(\mathbb{Q})}$ tiene una sola componente conexa. Ahora, si $S \subseteq \mathbb{R}^n$, tal que $\overline{S} = C_1 \cup \cdots \cup C_n$ con $C_i \neq \emptyset$ conexo, entonces la proyección en la componente i-ésima de S, $\rho_i(S)$ no puede ser el conjunto de los números enteros. En efecto, $\rho_i\left(\overline{S}\right) = \rho_i(\cup C_j) = \cup \rho_i(C_j)$ y como ρ_i es una función continua $\rho_i(C_j)$ es un subconjunto conexo de $\mathbb{R}$ y así $\overline{\rho(C_j)}$ también lo es. Además, como ρ es continua $\overline{\rho_i\left(\overline{S}\right)} = \overline{\rho_i(S)}$. Luego, si $\rho_i(S) = \mathbb{Z}$, entonces $\overline{\rho_i\left(\overline{S}\right)} = \overline{\rho_i(S)} = \overline{\mathbb{Z}} = \mathbb{Z}$, lo cual es absurdo ya que $\mathbb{Z}$ tiene infinitas componentes conexas.

Veamos que la conjetura de Mazur implica que $\mathbb{Z}$ no es diofantino en $\mathbb{Q}$. Supongamos por el absurdo que existe una ecuación $P(x, x_1, \ldots, x_{n-1}) = 0$ que define diofantinamente a $\mathbb{Z}$ en $\mathbb{Q}$, es decir, supongamos que la proyección en la primera componente de la variedad V cortada por P, sobre $\mathbb{Q}^n$, es el conjunto de los números enteros. Entonces haciendo $S = V(\mathbb{Q})$ tendríamos, en virtud de la conjetura de Mazur, que $\overline{S}$ tiene finitas componetes conexas, luego de lo anterior concluimos que $\rho_1(S) \neq \mathbb{Z}$, lo cual es absurdo.

Se podría pensar que la razón por la cual $\overline{V(\mathbb{Q})}$ debe tener sólo finitas componentes conexas se debe a que $\mathbb{Q}^n$ es denso en $\mathbb{R}^n$, es decir, que la verdad de la conjetura radica en algo topológico más que en algo aritmético. La siguiente proposición nos brinda evidencia en contra de esta afirmación.

Proposición 3.1.6 *$\mathbb{Z}$ es un subconjunto diofantino de* $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{m}{2^i} \mid m, i \in \mathbb{Z}\right\}$.

Prueba. Este proposición es una manera de refrasear el teorema 3.1.4 ya que para $x \in \mathbb{Z}\left[\frac{1}{2}\right]$, se cumple, en virtud de este teorema, que

$$x \in \mathbb{Z} \Leftrightarrow \left(\exists a, b, c \in \mathbb{Z}\left[\frac{1}{2}\right]\right)\left(7x^2 + 2 = a^2 + b^2 + c^2\right).$$

■

Notemos que $\mathbb{Z}\left[\frac{1}{2}\right]$ es denso en $\mathbb{R}$. Sin embargo, la superficie

$$V(\mathbb{R}) = \left\{(x, a, b, c) \in \mathbb{R} \mid 7x^2 + 2 - a^2 - b^2 - c^2 = 0\right\}$$

tiene infinitas componentes conexas, ya que su proyección en la primera componente es $\mathbb{Z}$. Además, aritméticamente hablando, $\mathbb{Z}\left[\frac{1}{2}\right]$ es muy diferente a $\mathbb{Q}$. De otra parte, con el objetivo de demostrar la insolubilidad de $H10(\mathbb{Q})$ se ha modificado ligeramente la noción de conjunto diofantino por la noción de modelo diofantino.

Definición 3.1.1 *Un modelo diofantino de $\mathbb{Z}$ sobre $\mathbb{Q}$ es un conjunto $S \subseteq X(\mathbb{Q})$, para algún conjunto diofantino X sobre $\mathbb{Q}$, equipado con una biyección $\phi : \mathbb{Z} \to S$ tal que las gráficas de la suma y multiplicación $\left(\subseteq \mathbb{Z}^3\right)$ corresponden a subconjuntos diofantinos de $S^3 \subseteq X^3(\mathbb{Q})$.*

Informalmente, un modelo diofantino de $\mathbb{Z}$ sobre $\mathbb{Q}$ es una copia de $\mathbb{Z}$ contenida en $\mathbb{Q}$, pero no de la manera estándar, sino de manera diofantina. Finalmente, antes de enunciar el resultado de Ponnen, recordemos que si $M \subseteq \mathcal{P}$, ($\mathcal{P}$ denota el conjunto de los números primos) entonces la densidad natural de M en $\mathcal{P}$ se define como el siguiente límite, cuando éste exista

$$\lim_{x\to\infty} \frac{\#\{p \in M \mid p \leq x\}}{\#\{p \in \mathcal{P} \mid p \leq x\}}.$$

Además, es importante notar que los subanillos de $\mathbb{Q}$ son de la forma $\mathbb{Z}\left[S^{-1}\right]$ (el menor anillo dentro de $\mathbb{Q}$ que contiene a $\mathbb{Z}$ y a los inversos multiplicativos de S), donde S es un subconjunto de los números primos.

En el 2002 Ponnen [20] demostró el siguiente teorema, el cual contrasta varias cosas vista en esta sección.

Teorema 3.1.7 *Existen conjunto disjuntos de primos $T_1, T_2 \subseteq \mathcal{P}$ con densidad natural igual a cero y tales que si $T_1 \subseteq S \subseteq \mathcal{P} - T_2$ entonces*

a) Existe una curva afin E' sobre $\mathbb{Z}\left[S^{-1}\right]$ tal que la clausura de $E'\left(\mathbb{Z}\left[S^{-1}\right]\right)$ en $E'(\mathbb{R})$ tiene infinitas componentes conexas.

b)Existe un modelo diofantino de $\mathbb{Z}$ sobre $\mathbb{Z}\left[S^{-1}\right]$ (definición análoga a la Definición 3.1.1).

c) $H10\left(\mathbb{Z}\left[S^{-1}\right]\right)$ es insoluble.

La prueba del teorema anterior utiliza varias técnicas de la aritmética de las curvas elípticas y es el primer ejemplo donde S es infinito.

También es posible mostrar que la conjetura de Mazur implica la no existencia de un modelo diofantino de $\mathbb{Z}$ sobre $\mathbb{Q}$. En general se conocen las siguientes implicaciones:

$\mathbb{Z}$ es diofantino sobre $\mathbb{Q}$	$\Rightarrow$	Existe un modelo diofantino de $\mathbb{Z}$ en $\mathbb{Q}$
$\Downarrow$	$\swarrow$	$\Downarrow$
La conjetura de Mazur es falsa		$H10(\mathbb{Q})$ es insoluble

Se espera que lo mostrado en esta sección explique un poco el porque $H10(\mathbb{Q})$ es el problema más destacado en esta área.

3.2 Lista de Resultados

En esta sección presentaremos una lista de los resultados conocidos sobre varios anillos R, sobre la (in)solubilidad de tanto la teoría de primer orden sobre R como $H10(R)$. Como es usual, $\mathbb{Q}_p$ denota el campo de los números p-ádicos (el campo de fracciones de la completación de $\mathbb{Z}_{(\langle p \rangle)}$

con respecto al ideal primo $\langle p \rangle$), F_q es el campo finito con q elementos (q es la potencia de un primo). Un campo de número es una extensión finita K de $\mathbb{Q}$ dentro de los complejos, O_k es la clausura entera de $\mathbb{Z}$ en K, es decir, el anillo de elementos de K que satisfacen un polinomio diofantino mónico. Un campo global de funciones es una extención finita del campo de funciones racionales $F_p(t)$, para algún primo p y donde t es indeterminada. Un campo p-ádico es una extensión finita de $\mathbb{Q}_p$, para algún p. μ_q denota un generador del grupo multiplicativo de F_q. En la siguiente tabla, la palabra "si" o "no" denotará solubilidad o insolubilidad de $H10(R)$ o de la teoría de primer orden sobre R. Es importante resaltar que el décimo problema de Hilbert sobre un campo de número arbitrario está abierta, sin embargo en todos los casos conocidos la respuesta ha sido negativa. Además, es claro que si la teoría de primer orden, sobre R, es decidible entonces $H10(R)$ también lo será. Por otra parte, si $H10(R)$ es insoluble entonces, con mayor razón, la teoría sobre R también lo será. Por último $F_q((t))$ denota el anillo de series formales en la variable t con coeficientes en F_q.

Anillo R	Lenguaje	Teoría de primer orden	Coef.	$H10(R)$
$\mathbb{C}$	$\{+,\cdot,0,1\}$	Sí (Elimin. de cuanti.)	$\mathbb{Z}$	Sí
$\mathbb{R}$	$\{+,\cdot,0,1\}$	Sí [27]	$\mathbb{Z}$	Sí
F_q	$\{+,\cdot,0,1\}$	Sí (Trivial)	$\mathbb{Z}$	Sí
Campos p-ádicos	$\{+,\cdot,0,1\}$	Sí [1], [7]	$\mathbb{Z}$	Sí [15]
$F_q((t))$	$\{+,\cdot,0,1,t,\mu_q\}$	Sin resolver.	$\mathbb{Z}[t,\mu_p]$	Sin resolver
Cam. de número K	$\{+,\cdot,0,1\}$	No [22]	$\mathbb{Z}$	Sin resolver
$\mathbb{Q}$	$\{+,\cdot,0,1\}$	No [23]	$\mathbb{Z}$	Sin resolver!!
Cam. glob. de func.	$\{+,\cdot,0,1,t,\mu_q\}$	No	$\mathbb{Z}[t,\mu_p]$	No [24], [6]
$F_q(t)$	$\{+,\cdot,0,1,t,\mu_q\}$	No [8], [16]	$\mathbb{Z}[t,\mu_p]$	No [19], [28]
$\mathbb{C}(t)$	$\{+,\cdot,0,1,t\}$	Sin resolver.	$\mathbb{Z}[t]$	Sin resolver
$\mathbb{C}(t,u)$	$\{+,\cdot,0,1,t,u\}$	No	$\mathbb{Z}[t,u]$	No [10]
$\mathbb{R}(t)$	$\{+,\cdot,0,1,t\}$	No	$\mathbb{Z}[t]$	No [3]
O_k	$\{+,\cdot,0,1\}$	No [22] Corolario	$\mathbb{Z}$	Sin resolver
$\mathbb{Z}$	$\{+,\cdot,0,1\}$	No (Teorema de Gödel)	$\mathbb{Z}$	No [13]

Tabla 1

En la Tabla 1 los anillos están agrupados de la siguiente manera: campos arquimedianos, campos finitos, campos locales no arquimedianos, campos globales, campos de funciones sobre campos arquimedianos y anillos de enteros. Estos están organizados de manera creciente con respecto a su "complejidad aritmética". No existe una noción precisa de complejidad aritmética, en el fondo lo que se quiere es tener un medidor de qué tan lejos estamos de entender la estructura. Por ejemplo, en el caso de campos, un buen indicador es el tamaño del grupo de Galois $G(K^s/K)$, donde K^s es la clausura separable de K. Además, aunque pueda parecer

extraño, los campos globales de funciones se consideran aritméticamente más complejos que los campos de número, ya que los primeros tienen una estructura aritmética extra, la cual proviene del automorfismo de Frobenius. En todos los casos conocidos el Automorfismo de Frobenius se ha usado para probar la indecibilidad sobr estos campos. Los dominios se consideran más complejos que sus campos de fracciones ya que los primeros tiene una estructura extra con respecto a los segundos, la relación de divisibilidad. La Tabla 1 muestra por una parte lo activa que es esta área en la actualidad y los diferentes temas que están implicados; y por otra parte todo lo que falta por investigar.

Finalmente, esperamos que este resumen incentive al interés del lector a hacer un estudio posterior en este bellísimo tema.

Bibliografía

[1] J. Ax y S. Kochen, Diophantine problems over local fields. III Decidable fields, Ann. of Math 83, 1966, 437-456

[2] M. Davis, On the number of solutions of diophantine ecuations, Proc. Amer. Math. Soc., 35 (1972) 552-554.

[3] J. Denef, The diophantine problem for polinomial rings and fields of rational functions, Trans Amer Math Soc, Providence RI, 200, 256-260

[4] J. Denef, Hilbert's tenth problem for quadratic rings, Proc. Amer. Math. Soc. Vol. 48, No 1, 214-220

[5] J. Denef, L. Lipshitz, F. Pheidas y J. V. Geel (editores) Hilbert's tenth problem: Relations with arithmetic and algebraic geometry, Amer. Math. Soc. Providence R.I., 2000

[6] K. Eisenträger, Hilbert's tenth problem for algebraic function fields of characteristic 2, Pacific J. Math, 2002

[7] Ju. L. Ersov, On the elementary theory of maximal normed fields, Dokl, Akad. Vauk SSSR 165 (1965), 21-23, Traducido al inglés en Soviet Math Dokl 6 (1965), 1930-1393

[8] Ju. L. Ersov, The undecidability of certain fields, Dokl Akad. Navk SSSR 162, 1965, 27-29

[9] J. P. Jones, Y. V. Matiyasevich, Proof of the recursive unsolvability of Hilbert's tenth problem, Amer. Math. Monthly, 98(8):689-709, 1991

[10] K. H. Klim y F. W. Roush, Diophantine undecidability of $\mathbb{C}(t_1, t_2)$, J. Algebra 150 (1992), No.1, 606-610

[11] D. Marker, Modern theory: An introduction, Springer Verlag, 2002

[12] Y. V. Matiyasevich, Enumerable sets are diophantine, Doklady Akademii Nauk SSSR, 191 (1970), 279-282. English translation with addendum, Soviet Mathematics; Doklady, 11 (1970), 354-357, MR 41,#3390.

[13] Ju. V. Matiyasevich, The diophantiness of enumerable sets, Dokl Akad Nauk SSSR 191 (1970), 279-282

[14] M. Minsky, Computation. Finite and infinite machines, Prentice-Hall, Englewood Cliffs, New Jersey, 1967, MR 50, #9050.

[15] A. Nerodic, A decision method for p-adic integral zeros of diophantine ecuations, Bulletin of the Amer. Math, Soc 69, 1963.

[16] Ju. G. Penzin, Undecidability of fields of rational functions over fields of characteristic 2, Algebra i logika, 12 (1973), 205-210

[17] T. Pheidas, Endomorphisms of elliptic curves and undecidability in function fields of positive characteristic, Journal of Algebra 273, 2004

[18] T. Pheidas, Extensions of Hilbert's tenth problem, Journal of symbolic logic, vol 54 N. 2 (1944) 372-397

[19] T. Pheidas, Hilbert's tenth problem for fields of rational functions over finite fields, Invent Math. 103, 1994, No 1, 1-8

[20] B. Poonen, Hilbert's tenth problem and Mazur's conjeture over large subrings of $\mathbb{Q}$, 2002, http://math.berkeley.edu/poonen/papers

[21] J. Robinson, Existencial definability in arithmetic, Trans. Amer. Math. Soc., 72 (1452), 437-449, MR 14, #4.

[22] J. Robinson, The undecidability of algebraic rings and fields, Proc. Amer. Math soc. 10 (1959), 950-957

[23] J. Robinson, Definability and decision problems in arithmetic, J. Symbolic logic 14 (1949) 98-114

[24] A. Shlapentokh, Hilbert's tenth problem for rings of algebraic functions in one variable over fields of constants of positive characteristic, Trans Amer. Math. Soc. 333, 1992, No,1, 275-298

[25] J. Silverman, The arithmetic of elliptic curves, Springer Verlag, New York, 1986

[26] J. Silverman, J. Tate, Rational points on elliptic curves.

[27] A. Tarski, A decision method for elementary algebra and geometry, University of California press, Berkeley and Los Angeles, Calif 1957, 2nd ed.

[28] C. Videla, Hilbert's tenth problem for rational functions over fields of characteristic 2, Proc. Amer. Math. Soc. 120, 1994 No.1, 249-253

[29] C. Videla, El décimo problema de Hilbert, curvas elípticas y la conjetura de Mazur, Cursillo dictado en el XV Congreso Nacional de Matemáticas, Bogotá, Agosto 8-12 2005, Memorias del congreos, por aparecer.

[30] K. Zahidi, On diofantine sets over polinomial rings, Proc. Amer. Math. Soc. Vol 128, No.3, 877-884