Sociedad Colombiana de Matemáticas
XV Congreso Nacional de Matemáticas
2005 **Apuntes**

Lecturas Matemáticas
Volumen Especial (2006), páginas 185–209

El décimo problema de Hilbert, curvas elípticas y la conjetura de Mazur

Carlos R. Videla
CINVESTAV–IPN, México D.F., México

Abstract. An elementary introduction to the use of the arithmetic of elliptic curves in showing the unsolvability of logic theories is presented. The works of Pheidas and Mazur on Hilbert's 10^{th} problem over $\mathbb{Q}$ are explained.

Key words and phrases. Hilbert's 10^{th} problem, Elliptic curves, Mazur's conjecture, Logic.

2000 AMS Mathematics Subject Classification. 03C60, 03C62, 11G05, 12L12, 14H53.

Resumen. Se presenta una introducción elemental al uso de la aritmética de curvas elípticas para demostrar la insolubilidad de teorías lógicas. Se explican los trabajos de Pheidas y de Mazur sobre el décimo problema de Hilbert en $\mathbb{Q}$.

1. Introducción.

El propósito de este cursillo es el de presentar una introducción elemental al uso de la aritmética de curvas elípticas para demostrar la insolubilidad de teorías lógicas. La razón por la cual elegí este tema es porque la posible solución negativa al décimo problema de Hilbert sobre $\mathbb{Q}$ depende de si existen curvas elípticas definidas sobre $\mathbb{Q}$ con ciertas propiedades aritméticas. Este proyecto lo explicó Pheidas en 1998 (ver [5]). No abordaré el trabajo de Pheidas pues requiere conocimientos más avanzados.

El pionero en el uso de curvas elípticas para demostrar insolubilidad fue Rafael Robinson. En 1950 demostró que la teoría elemental del campo $\mathbb{Q}(t)$ es insoluble. Este resultado y una generalización posterior, son la parte principal de este cursillo. En otra dirección B. Mazur, reconocido especialista en curvas elípticas, hizo una conjetura en 1991 que implica que el programa

de PHEIDAS ¡no puede ser cierto! Esta conjetura es el tema de la sección 3 de estas notas. Hay pues incertidumbre: ¿quién tiene la razón?

Para mi fué muy grato el haber participado en la celebración de los 50 años de la Sociedad Colombiana de Matemáticas. Le agradezco a los profesores LUIS J. CORREDOR, XAVIER CAICEDO y ANDRES VILLAVECES la invitación que me hicieron.

2. **El décimo problema de Hilbert.**

El décimo problema de HILBERT original (abreviado $H10(\mathbb{Z})$) es:

"Dar un algoritmo que decida para cada ecuación

$$f(x_1, x_2, \ldots, x_n) = 0 \tag{1}$$

donde f es un polinomio con coeficientes en $\mathbb{Z}$, si tiene o no una solución con cada $x_i \in \mathbb{Z}$".

Este problema es el décimo en la famosa lista de 23 problemas que propuso HILBERT en 1900.

Resolver ecuaciones como (1) en enteros es un problema natural, extremadamente general, difícil y cuya solución en casos especiales ha producido teorías matemáticas bellísimas (y útiles en otros contextos).

Hay cierto enigma en la pregunta de HILBERT. Parece ser que HILBERT anticipa una solución positiva al problema. Por otro lado, es también natural preguntarse si (1) posee soluciones en $\mathbb{Q}$: ¿porqué HILBERT no hace ésta pregunta?

Note que $H10(\mathbb{Z})$ no pide encontrar las soluciones a (1); sólo decidir si las tiene o no. Evidentemente HILBERT reconoce aquí que encontrar las soluciones puede ser aún muchísimo más difícil.

El problema $H10(\mathbb{Z})$ es realmente monstruoso. Note que el problema incluye la solución a sistemas de ecuaciones pues si $f_1, f_2, \ldots, f_r$ pertenecen a $\mathbb{Z}[x_1, \ldots, x_n]$ entonces el sistema $f_1 = 0, f_2 = 0, \ldots, f_r = 0$ tiene solución en $\mathbb{Z}^n$ si y sólo si la ecuación $f_1^2 + f_1^2 + \cdots + f_r^2 = 0$ tiene solución en $\mathbb{Z}^n$.

¿Qué evidencia tenía HILBERT a su favor?

La generalización que más nos interesa es la siguiente:

¿Existe un algoritmo que para cada ecuación (1) decida si ésta posee soluciones con cada $x_i \in \mathbb{Q}$?

Abreviamos esta pregunta por $H10(\mathbb{Q})$. Nótese que para una ecuación fija, el que ésta no posea soluciones enteras no implica automáticamente que no las tenga racionales; y si tiene soluciones racionales ello no implica que se sepa algo sobre si tiene soluciones enteras o no.

Es probable que HILBERT conociera el siguiente resultado. Esto explicaría porque no formuló $H10(\mathbb{Q})$ separadamente.

Proposición 2.1. *Si $H10(\mathbb{Z})$ es soluble entonces $H10(\mathbb{Q})$ es soluble.*

Demostración. Sea $f \in \mathbb{Z}[x_1, \ldots, x_n]$. Existen $r_1, r_2, \ldots, r_n \in \mathbb{Q}$ y $f(r_1, \ldots, r_n) = 0(2) \Leftrightarrow$ existen $x_1, \ldots, x_n, z \in \mathbb{Z}$ con $f(\frac{x_1}{z}, \ldots, \frac{x_n}{z}) = 0$ y $z \neq 0 \Leftrightarrow$ existen $x_1, \ldots, x_n, z \in \mathbb{Z}$ con $z \neq 0$ y

$$z^d f(\frac{x_1}{z}, \ldots, \frac{x_n}{z}) = g(x_1, \ldots, x_n, z) = 0(2a)$$

(con $d =$ grado máximo de los monomios de f y $g \in \mathbb{Z}[x_1, \ldots, x_n, z]$).

Esto casi es suficiente. Falta expresar la condición $z \neq 0$ por medio de un polinomio. Esto se puede hacer de varias manera. Usamos una idea de Denef.

Lema 1. *$z \neq 0 \Leftrightarrow$ existen $a, b, \in \mathbb{Z}$ tales que $z = ab$ y $(a, 2) = 1$ y $(b, 3) = 1$ (aquí (x, y) es el máximo común divisor de x, y)*

Demostración (del lema). "$\Leftarrow$": Si $(a, 2) = 1$ entonces $a \neq 0$ y de igual modo si $(b, 3) = 1$ entonces $b \neq 0$. Luego $z = ab \neq 0$.

"$\Rightarrow$": Si $z \neq 0$ sea $z = (2^i x)(3^j y)$ con $i, j, \geq 0$, $2 \not| xy$, $3 \not| xy$. Sea $a = 3^i y$, $b = 2^i x$. Entonces $(a, 2) = 1$ y $(b, 3) = 1$. Recordamos ahora que para enteros x, y vale $(x, y) = 1$ si y sólo si existen enteros u, ω tales que

$$ux + \omega y = 1$$

Concluimos entonces que: $z \neq 0 \Leftrightarrow$ existen $a, b, c, d, e, f \in \mathbb{Z}$ con

$$\begin{aligned} z - ab &= 0 \\ 2c + ad - 1 &= 0 \\ 3e + bf - 1 &= 0 \end{aligned}$$

$\Leftrightarrow (z - ab)^2 + (2c + ad - 1)^2 + (3e + bf - 1)^2 = 0$ ☑

Continuando con la demostración de la proposición tenemos que

$$(2a) \Leftrightarrow \text{ existen } x_1, x_2, \ldots, x_n, z, a, b, c, d, e, f \in \mathbb{Z}$$

y

$$g(x_1, \ldots, x_n, z)^2 + (z - ab)^2 + (2c + ad - 1)^2 + (3e + bf - 1)^2 = 0 \quad (3)$$

Tenemos pues que (2) $\Leftrightarrow$ (3).

Sea P un programa para decidir $H10(\mathbb{Z})$. Entonces puedo usar ese mismo programa para resolver el $H10(\mathbb{Q})$: si P aplicado a (3) dice "si" entonces (2) es cierta. Si P aplicado a (3) dice "no" entonces (2) es falsa. ☑

Una pregunta natural es la siguiente: ¿Cuáles ecuaciones $f(x_1, \ldots, x_n) = 0$, con $f \in \mathbb{Z}[\vec{x}]$, son fáciles de decidir? Pensemos por el momento en soluciones enteras. Evidentemente si $f(\vec{x}) = 0$ tiene solución en $\mathbb{Z}^n$ entonces la tiene en $\mathbb{R}^n$ y, para cada entero $M > 1$ las congruencias $f(\vec{x}) \equiv \text{mod } (M)$ tienen solución. Por el teorema chino de los residuos las congruencias mod M se reducen a congruencias mod (p^n) para cada primo p y cada $n \geq 1$. Así, por ejemplo, la ecuación $y^2 = x^3 + 7$ no tiene soluciones enteras (sí las tiene en $\mathbb{R}$) porque

no hay soluciones a la congruencia $y^2 \equiv x^3 + 7 \bmod (M)$ para todo M. La condición de solubilidad real y las congruencias no son suficientes para forzar solubilidad en $\mathbb{Z}$. Por ejemplo, $10x^2 + 29x + 21 = (2x + 3)(5x + 7) = 0$ tiene soluciones en $\mathbb{R}$ y mod (p^n) para cada primo p y $n \geq 1$, pero no las tiene en $\mathbb{Z}$.

Es útil saber que resolver ecuaciones (con coeficientes en $\mathbb{Z}$) sobre $\mathbb{R}$ es algoritmicamente soluble (se deduce del teorema de TARSKI pero a lo mejor se conocia anteriormente). Para cada p y n fijos, decidir si $f(\vec{x}) \equiv 0 \bmod (p^n)$ tiene solución es en el peor de los casos una verificación finita. NERODE [4] demostró en 1963 el siguiente resultado: Sea p un primo dado. Existe un algoritmo que para cada ecuación $f(x_1, \ldots, x_n) = 0$ con $f \in \mathbb{Z}[\vec{x}]$ decide si las infinitas congruencias $f \equiv 0 \bmod p$, $f \equiv 0 \bmod p^2$, etc. tienen o no solución.

Esto es un buen avance pero hay infinitos primos que verificar. AX en 1967 [1] demostró que existe un algoritmo que para cada ecuación decide si hay solución a la congruencia $\bmod(p^n)$ para todo primo p y $n \geq 1$. El ejemplo anterior $(10x^2 + 29x + 21 = 0)$ tiene soluciones en $\mathbb{Q}$. Uno podría pensar que las condiciones de solubilidad en $\mathbb{R}$ y de congruencia, si bien no implican una solución entera a lo mejor sí implican una solución en $\mathbb{Q}$. Esto no es cierto: la ecuación $(x^2-13)(x^2-17)(x^2-221) = 0$ tiene soluciones en $\mathbb{R}$ y $\bmod(p^n)$ para cada primo p y $n \geq 1$ pero claramente no en $\mathbb{Q}$.

Para resumir: por los teoremas de TARSKI y AX el conjunto de ecuaciones $f(\vec{x}) = 0$ con $f \in \mathbb{Z}[\vec{x}]$ que tienen soluciones reales y soluciones a cada congruencia $\bmod(M)$ $(M > 1)$ es recursivo. Las que tiene soluciones en $\mathbb{Z}$ son un subconjunto propio de éstas (recursivamente enumerable). En 1970 MATIJASEVIC mostró que $H10(\mathbb{Z})$ no es soluble.

Nadie sabe como invertir la implicación en la Proposición 2.1, así que el problema $H10(\mathbb{Q})$ esta abierto. ¡Un problema fascinante!

Es conveniente introducir la siguiente definición debida a M. DAVIS.

Definición 2.2. Sea R un subanillo de $\mathbb{Q}$: un subconjunto $S \subset R^n$ se llama *diofantino* si existe un polinomio $f(\vec{x}, \vec{y}) \in \mathbb{Z}[\vec{x}, \vec{y}]$ donde $\vec{x} \in R^n$ y $\vec{y} \in R^m$ tal que: $\vec{s} \in S \Leftrightarrow$ existe $\vec{w} \in R^m$ con $f(\vec{s}, \vec{w}) = 0$.

En términos geométricos S es la proyección en R^n del conjunto algebraico $f(\vec{x}, \vec{y}) = 0$ en R^{n+m}. Existe una especie de álgebra de conjuntos diofantinos. En lo que sigue usaremos el símbolo $\exists$ para abreviar "existe".

Lema 2. *Si $A, B \subset R^n$ son diofantinos entonces $A \cup B$ y $A \cap B$ son diofantinos.*

Demostración. Si $\vec{a} \in A \Leftrightarrow \exists \vec{y} \in R^m (f(\vec{a}, \vec{y}) = 0)$ y $\vec{b} \in B \Leftrightarrow \exists \vec{\omega} \in R^p (g(\vec{b}, \vec{\omega}) = 0)$, entonces:

$$\begin{aligned} \vec{x} \in A \cap B &\Leftrightarrow \exists \vec{y}, \vec{\omega} (f(\vec{x}, \vec{y})^2 + g(\vec{x}, \vec{\omega})^2 = 0) \\ \vec{c} \in A \cup B &\Leftrightarrow \exists \vec{y}, \vec{\omega} (f(\vec{x}, \vec{y}) \cdot g(\vec{x}, \vec{\omega}) = 0). \end{aligned}$$ ☑

Ejemplos 2.3. a) $\mathbb{N} = \{0, 1, \ldots\} \subset \mathbb{Z}$ es diofantino en $\mathbb{Z}$. Por el teorema de Lagrange tenemos, $z \in \mathbb{N} \Leftrightarrow \exists a, b, c, d \in \mathbb{Z} (z = a^2 + b^2 + c^2 + d^2)$.

b) $A = \{z : z \neq 0\}$. Vimos anteriormente que A es diofantino en $\mathbb{Z}$.
c) $\mathbb{Q}^+ = \{r \geq 0 : r \in \mathbb{Q}\}$ es un subconjunto diofantino de $\mathbb{Q}$.

$$r \in \mathbb{Q}^+ \Leftrightarrow \exists a, b, c, d \in \mathbb{Q}(r = a^2 + b^2 + c^2 + d^2)$$

(ejercicio usando a)).
d) $B = \{(x, y) : x \text{ divide a } y\}$ es un subconjunto diofantino de $\mathbb{Z}^2$.

$$(a, b) \in B \Leftrightarrow \exists z \in \mathbb{Z}(b = z \cdot a).$$

Pregunta 2.4. ¿Es $\mathbb{Z}$ es un subconjunto diofantino de $\mathbb{Q}$?

Esta es una gran pregunta pues tenemos:

Corolario 1. *Si $\mathbb{Z}$ es diofantino entonces $H10(\mathbb{Q})$ es insoluble.*

Demostración. Sea $r \in \mathbb{Q}$ y supongamos que $r \in \mathbb{Z} \Leftrightarrow \exists \vec{y} \in \mathbb{Q}^n(f(r, \vec{y}) = 0)$. Entonces podemos reducir $H10(\mathbb{Z})$ a $H10(\mathbb{Q})$ así:

$$\exists x_1, \ldots, x_m \in \mathbb{Z} : g(x_1, \ldots, x_m) = 0 \tag{4}$$

$$\Leftrightarrow \quad \exists x_1, \ldots, x_m \exists \vec{y}_1, \ldots, \vec{y}_m \in \mathbb{Q} : \tag{5}$$
$$f(x_i, \vec{y}_i) = 0 \quad \text{para} \quad i = 1, \ldots, m \quad \text{y} \quad g(x_1, \ldots, x_m) = 0$$

$$\Leftrightarrow \quad \exists x_1, \ldots, x_m \exists \vec{y}_1, \ldots, \vec{y}_m \in \mathbb{Q} : \sum_{i=1}^{m} f(x_i, \vec{y}_i)^2 + g(\vec{x})^2 = 0 \tag{6}$$

Si P es un programa para decidir ecuaciones sobre $\mathbb{Q}$ entonces lo puedo usar para decidir ecuaciones sobre $\mathbb{Z}$, pues (4) $\Leftrightarrow$ (6). Esto contradice el teorema de Matijasevic. ☑

Hay un equivalente al $H10(\mathbb{Q})$ que es interesante. Antes de formularlo necesitamos una definición. Un polinomio $f \in \mathbb{Z}[x_1, \ldots, x_n]$ se llama homogéneo (o una forma) de grado d si cada monomio de f tiene grado d. Por ejemplo $f(x, y) = 3x^3 + xy^2$ es una forma en dos variables de grado 3. Para f homogéneo la ecuación $f = 0$ simpre tiene la solución trivial donde $x_i = 0$ para cada i. Una solución no trivial es por definición una solución donde al menos un $x_i \neq 0$. Para polinomios homogeneos la ecuación $f = 0$ posee soluciones enteras no triviales si y sólo si posee soluciones racionales no triviales.

Proposición 2.5. *El $H10(\mathbb{Q})$ es equivalente a decidir si ecuaciones homogéneas con coeficientes en $\mathbb{Z}$ poseen o no soluciones no triviales en $\mathbb{Z}$.*

Demostración. Seguimos una demostración dada por A. Adler. Primero reducimos $H10(\mathbb{Q})$ al problema sobre formas. Sea $P(x_1, \ldots, x_n) = 0$ una ecuación con coeficientes en $\mathbb{Z}$ y deseamos saber si tiene soluciones en $\mathbb{Q}^n$.

Sea $R(x_1, x_2, \ldots, x_n, u) = u^d P(\frac{x_1}{u}, \ldots, \frac{x_n}{u})$ la homogenización de P donde $d =$ grado de $P =$ grado máximo de los monomios de P. Defina

$$S(x_1, \ldots, x_n, r_1, \cdot, r_4, y) = \sum_{i=1}^{n} x_i^2 + \sum_{i=1}^{4} r_i^2 - y^2 \text{ y } T(y, z, u) = y^2 - 2z^2 - u^2.$$

Note que $P = 0$ tiene solución en $\mathbb{Q}^n \Leftrightarrow R = 0$ tiene solución en enteros x_i, u con $u \neq 0$. Sea $D = R^4 + S^{2d} + T^{2d}$. Entonces D es una forma de grado $4d$ en $n + 7$ variables con coeficientes en $\mathbb{Z}$.

Vale lo siguiente:

$$P = 0 \text{ tiene solución en } \mathbb{Q}^n \Leftrightarrow D = 0 \quad \text{tiene solución no trivial en } \mathbb{Z}^n (\text{o } \mathbb{Q}^n).$$

Antes de demostrar esta afirmación necesitamos un lema sobre $\sqrt{2}$.

Lema 3. *La ecuación $x^2 - 2y^2 = 1$ tiene infinitas soluciones.*

Demostración. El par $(3, 2)$ es una solución. Obtenemos más usando la norma de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$: para $\alpha = x + \sqrt{2}y$ con $x, y \in \mathbb{Z}$ defina

$$\begin{aligned} N(\alpha) &= (x + \sqrt{2}y)(x - \sqrt{2}y) \\ &= x^2 - 2y^2 \,. \end{aligned}$$

Es fácil probar que $N(\alpha\beta) = N(\alpha)N(\beta)$ (donde $\beta = u + \sqrt{2}v$ con $u, v, \in \mathbb{Z}$). Se deduce de esto que si $N(\alpha) = 1$ entonces $N(\alpha^2) = N(\alpha^3) = \cdots = 1$. Tomando $\alpha = 3 + \sqrt{2} \cdot 2$ tenemos $N(\alpha) = 1$ luego $N(\alpha^n) = N(x_n + \sqrt{2}y_n) = 1$ con $x_n, y_n \in \mathbb{Z}$ para cada $n \geq 1$. La última ecuación dice que $x_n^2 - 2y_n^2 = 1$. Como $\alpha^n \neq \alpha^m$ para $n \neq m$, tenemos infinitas soluciones. Ciertamente entonces $|x_n| \to \infty$. ☑

El lema será usando de la siguiente forma: para $a \neq 0$ en $\mathbb{Z}$ la ecuación

$$x^2 - 2y^2 = a^2$$

tiene soluciones con x^2 arbitrariamente grande. Esto es inmediato pues podemos tomar un par (x_n, y_n) con x_n^2 arbitrariamente grande y $x_n^2 - 2y_n^2 = 1$. Entonces tenemos $(ax_n)^2 - 2(ay_n)^2 = a^2$ con $(ax_n)^2$ arbitrariamente grande. Volviendo a la demostración de la proposición supongamos que $P = 0$ tiene solución en $\mathbb{Q}^n$. Entonces $R(\vec{x}, u) = 0$ con $u \neq 0$. Ahora, $y^2 - 2z^2 = u^2$ tiene soluciones con $y^2 \geq \sum_{i=1}^{n} x_i^2$. Por el teorema de Lagrange existen r_1, r_2, r_3, r_4 en $\mathbb{Z}$ tales que $\sum_{i=1}^{n} x_i^2 - y^2 + \sum_{i=1}^{n} r_i^2 = 0$. Luego $R = 0, T = 0$ y $S = 0$. Es decir $D = 0$.

En la otra dirección, supongamos que $D(\vec{x}, \vec{r}, u, y, z) = 0$ con alguna variable no nula.

Si $y = 0$, puesto que $R = T = S = 0$, tenemos $z = 0$, $u = 0$, $\vec{r} = 0$ y $\vec{x} = 0$.

Concluimos que $y \neq 0$. Puesto que $\sqrt{2} \notin \mathbb{Q}$ se sigue que $u \neq 0$ y tenemos que $R = 0$ y $u \neq 0$. Luego $P = 0$.

En la otra dirección, supongamos que $f(x_1, \ldots, x_n)$ es una forma de grado d y que queremos saber si existen soluciones enteras no triviales a $f(\vec{x}) = 0$. Dejamos como ejercicio verificar que esto ocurre si y sólo si $g(x_1, \ldots, x_n) = f(1, x_2, \ldots, x_n) \cdots f(x_1, x_2, \ldots, 1) = 0$ tiene soluciones en $\mathbb{Q}$. ☑

La proposición 2.5 es interesante porque es un hecho empírico que hay más métodos para demostrar teoremas sobre formas que sobre polinomios no homogéneos. Por otro lado, hay un fenomeno interesante: formas con muchas variables con respecto a su grado automáticamente tienen soluciones no triviales en $\mathbb{Q}$. Por ejemplo, Meyer en 1884 demostró que una forma cuadrática en 5 o más variables con coeficientes enteros tiene una solución no trivial en $\mathbb{Z}$ si es indefinida (es decir si tiene una solución no trivial en $\mathbb{R}$). La condición de ser indefinida es claramente necesaria pues las formas $f : \sum_{i=1}^{n} a_i x_i^2$ con $a_i > 0$ no tiene soluciones no triviales para ningún $n \geq 1$. De hecho para formas cuadráticas vale el famoso resultado de Hasse–Minkowski: una forma cuadrática tiene soluciones no triviales en $\mathbb{Q}$ si y sólo si tiene tales soluciones en $\mathbb{R}$ y mod (M) para todo $M > 1$. En particular esto implica que podemos decidir para una forma cuadrática si ésta posee soluciones no–triviales. Por peculiaridades del caso cuadrático ("completar el cuadrado") esto implica que podemos decidir si un polinomio no homogéneo de grado 2 en cualquier número de variables tiene una raíz en $\mathbb{Q}$ (o en $\mathbb{Z}$). El caso de formas cúbicas esta abierto y la matemática que ha generado es espectacular. Un resultado hermoso es el de Davenport de 1963 que no ha sido mejorado: Toda forma cúbica con coeficientes en $\mathbb{Z}$ tiene una solución no trivial en $\mathbb{Q}$ si tiene 16 o más variables. Se piensa que 10 debe ser suficiente. La investigación diofantina de las cúbicas todavía da para muchos años más.

Otro resultado en esta misma dirección es el teorema de Birch: Si $d \geq 1$ es 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 $\mathbb{Q}$. En vista de la proposición 2.5 estos resultados muestran que hay grandes familias de ecuaciones que tiene soluciones racionales. Obviamente no hay problema para decidir estas ecuaciones. ¿Es de locos pensar que $H10(\mathbb{Q})$ es soluble?

Un intento para responder la pregunta 2.4 es la de eliminar denominadores de un número racional r de manera diofantina. A continuación mostraremos como J. Robinson y R. Robinson usaron un teorema de Gauss para eliminar el primo 2.

Teorema 2.6. [Gauss 1800]. *Sea* $m \geq 1$, $m = 4^n \cdot u$, $4 \nmid u$. *Entonces* $\exists x, y, z \in \mathbb{Z}$ *tales que* $x^2 + y^2 + z^2 = m \not\equiv 7 \mod 8$

Corolario 2. *Sea* $m \in \mathbb{Z}$. *Entonces* $\exists p, q, r \in \mathbb{Q}$ *tales que* $p^2 + q^2 + r^2 = m \Leftrightarrow$ $\exists x, y, z \in \mathbb{Z}$ *con* $x^2 + y^2 + z^2 = m$.

No haremos la demostración del teorema, pero si la del corolario.

Demostración. Suponga $p = \dfrac{a}{b}, q = \dfrac{c}{d}$ y $r = \dfrac{e}{f}$. Esto implica que

$$(adf)^2 + (cbf)^2 + (ebf)^2 = m(dbf)^2.$$

Pongamos $m = 4^n u$ con $4 \nmid u$. Tenemos que mostrar que $u \not\equiv 7 \bmod (8)$.

Sea $bdf = 4^m v$ con $4 \nmid v$. Esto implica que $m(bdf)^2 = 4^{n+2m} uv^2$. Aplicando el teorema a este número vamos a concluir que $u \not\equiv 7 \bmod (8)$. Esto lo hacemos investigando la paridad de v:

Caso I: Suponga $4 \nmid uv^2$, luego por el teorema $uv^2 \not\equiv 7 \mod (8)$. Por otro lado, $v \equiv 1, 3, 5, 7 \bmod(8)$ y entonces $v^2 \equiv 1 \bmod(8)$ (vea la tabla más adelante).

Si $u \equiv 7 \bmod(8)$ entonces $uv^2 \equiv 7 \bmod(8)$ lo cual es imposible. Concluímos que $u \not\equiv 7 \mod (8)$ y por el teorema m es la suma de tres cuadrados enteros.

Caso II: Si $v \equiv 0 \bmod(2)$ (pero $\not\equiv 0 \bmod(4)$). Entonces $v = 2s$ con $s \equiv 1 \bmod(2)$. Se sigue que $m(bdf)^2 = 4^{n+2m+1} \cdot us^2$ con $4 \nmid us^2$. Como antes $us^2 \not\equiv 7 \mod (8)$. Como $s \equiv 1 \bmod(2)$, $s^2 \equiv 1 \bmod(8)$. Igual que en el Caso I concluimos que $u \not\equiv 7 \mod (8)$. Esto término la demostración. ☑

La tabla que sigue será útil en la demostración del teorema 2.8. En ella todos los valores son calculados mod(8).

2.7. **Tabla.**

x	x^2	$7x^2$	$7x^2+2$
0	0	0	2
1	1	7	1
2	4	4	6
3	1	7	1
4	0	0	2
5	1	7	1
6	4	4	6
7	1	7	1

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

Teorema 2.8. *R es un subconjunto diofantino de $\mathbb{Q}$. Tenemos la siguiente definición: para $x \in \mathbb{Q}$,*

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

Demostración. "$\Leftarrow$": Supongamos que $x, a, b, c \in \mathbb{Q}$ y $7x^2 + 2 = a^2 + b^2 + c^2$, y que $x = \dfrac{n}{2^t m}$ con $(n, m) = 1, 2 \not| n, 2 \not| m$ y $t \geq 1$. Eliminando denominadores del lado izquierdo tenemos

$$7n^2 + 2 \cdot 2^{2t} m^2 = \text{ suma de tres cuadrados de } \mathbb{Q}.$$

Por el corolario podemos tomar los cuadrados en $\mathbb{Z}$ (es decir cuadrados de números enteros). Como n es impar tenemos según la tabla que $7n^2 + 2 \cdot 2^{2t} \cdot m^2 \equiv 7n^2 \equiv 7 \bmod(8)$. De ahí que $7n^2 + 2 \cdot 2^{2t} \cdot m = 7 + 8k$ para algún k entero. Ahora, los números de la forma $7 + 8k$ son de la forma $4^0 \cdot u$, $4 \not| u$. Pero entonces $u \equiv 7 \bmod(8)$ lo cual contradice el teorema de GAUSS.

"⇒". Sea $x = \dfrac{n}{m}$ con $(n, m) = (2, m) = 1$. Entonces $7x^2 + 2$ es suma de tres cuadrados si y sólo si $7n^2 + 2m^2$ es suma de tres cuadrados. Y esto último es cierto si y sólo si $7n^2 + 2m^2$ no es de la forma $4^s(8k + 7)$. Probamos esto por contradicción:

Caso I: $s \geq 1$. Tenemos que $2|7n^2$ luego $4|7n^2$. Como $4|7n^2 + 2m^2$ tenemos que $4|2m^2$ luego m es par. Esto es una contradicción.

Caso II: $s = 0$. Aquí $7n^2 + 2m^2 = 8k + 7$.

Esto quiere decir que $7n^2 + 2m^2 \equiv 7 \bmod(8)$. Como m es impar, de la tabla concluímos que $2m^2 \equiv 2 \bmod(8)$. Otra vez, usando la tabla, vemos que $7n^2 + 2m^2 \not\equiv 7 \bmod(8)$.

Contradicción. En conclusión, $7n^2 + 2m^2$ no es de la forma $4^s(8k + 7)$ luego por el teorema de Gauss $7x^2 + 2$ es la suma de tres cuadrados. ☑

Julia Robinson en 1949 encontró cómo eliminar cada primo p del denominador. Si $f(x, y, z, a, b, c) = x^2 + ay^2 - bz^2 - abc^2 - 2$, demostró que para cada primo p existen enteros a_p, b_p tales que la proyección sobre c del conjunto en $\mathbb{Q}^4$ definido por $f(x, y, z, a_p, b_p, c) = 0$ es exactamente el subanillo de $\mathbb{Q}$ que consta de racionales $\dfrac{m}{n}, (m, n) = 1$ y $p \nmid n$. Como la intersección finita de conjuntos diofantinos es diofantino tenemos que el anillo

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

es diofantino en $\mathbb{Q}$ para cada conjunto finito S de números primos.

Todavía estamos infinitamente lejos de $\mathbb{Z}$. Sólo en 2003, sorprendentemente, Poonen logró mejorar estos resultados (ver la nota que sigue a 3.3).

J. Robinson logró usar sus formas cuadráticas para demostrar que la teoría elemental de $\mathbb{Q}$ es insoluble. Este resultado será discutido en la Sección 5.

3. La conjetura de B. Mazur

En 1990 B. Mazur hizo la siguiente conjetura ([3]):

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

Aquí $V(\mathbb{Q}) = V \cap \mathbb{Q}^n$, por definición. También note que se sabe que V tiene un número finito de componentes conexas.

3.1. Ejemplos simples.

a) Sea $V : y - x^2 = 0$
   V es la bien conocida parabola.
   V tiene una sola componente conexa.

$V(\mathbb{Q})$ es un subconjunto de V y su gráfica la varíamos como una nube de puntos con muchos huecos. Obviamente $V(\mathbb{Q}) = \{(r, r^2) : r \in \mathbb{Q}\}$. Luego tenemos $\overline{V(\mathbb{Q})} = V$. Luego $\overline{V(\mathbb{Q})}$ tiene una componente conexa. En general esto vale para $V : y - p(x) = 0$ con $p(x) \in \mathbb{Q}[x]$.

b) $V : y^2 = x^3$

Aquí V tiene una sola componente.

¿Como es $V(\mathbb{Q})$? Observe que para $r \in \mathbb{Q}$, $(r^2, r^3) \in V(\mathbb{Q})$. Ahora si $(\alpha, \beta) \in V(\mathbb{R})$ buscamos r racional con $r^2 \approx \alpha$ y entonces $r^3 \approx \alpha^{3/2} = \beta$; tenemos que $\overline{V(\mathbb{Q})} = V$

c) $V : x^4 + y^4 - 1 = 0$

V tiene otra vez una sola componente.

Fermat demostró que $V(\mathbb{Q}) = \{(0, \pm 1), (\pm 1, 0)\}$. Luego $\overline{V(\mathbb{Q})}$ tiene cuatro componentes.

d) $V : y^2 - x^3 + 4 = 0$

V tiene una sola componente. Un resultado no trivial es que $\overline{V(\mathbb{Q})} = V$. Vea 4.4.

La razón fundamental por la cual MAZUR hizo la conjetura es porque él no cree que $\mathbb{Z}$ es un subconjunto diofantino de $\mathbb{Q}$. Esto se deduce del siguiente resultado.

Lema 4. *Sea $S \subset \mathbb{R}^n$ y supongamos $\overline{S} = C_1 \cup C_2 \cup \cdots \cup C_n$ cada $C_i \neq \phi$, conexo. Entonces $p(S) \neq \mathbb{Z}$ (donde p es la proyección en una de las coordenadas).*

Demostración. Tenemos

$$p(\overline{S}) = p(\cup C_i) = \cup p(C_i).$$

Como p es continua $p(C_i)$ es un subconjunto conexo de $\mathbb{R}$. También $\overline{p(C_i)}$ es conexo. Tenemos entonces que $\overline{p(\overline{S})} = \cup \overline{p(C_i)}$; luego $\overline{p(\overline{S})}$ tiene a lo sumo n componentes conexas. Ahora, para f continua, $f : X \to Y$ vale $\overline{f(\overline{X})} = \overline{f(X)}$. Aplicando esto a la proyección p tenemos $\overline{p(\overline{S})} = \overline{p(S)}$. Si $p(S) = \mathbb{Z}$ tendríamos, por lo de arriba, que $\overline{p(S)} = \overline{\mathbb{Z}} = \mathbb{Z}$ tiene a lo sumo n componentes conexas, lo cual es falso. ☑

Se podía 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. Observe que esto no puede ser así:

Proposición 3.2. *$\mathbb{Z}$ es un subconjunto diofantino de*

$$\mathbb{Z}[\frac{1}{2}] = \{\frac{m}{2^t} : t \geq 0, m \in \mathbb{Z}\}.$$

Demostración. Ya lo hicimos en la Sección 2. Para $x \in \mathbb{Z}[\frac{1}{2}]$:

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

Note que $\mathbb{Z}\left[\frac{1}{2}\right]$ es denso en $\mathbb{R}$. Sin embargo la superficie en $\mathbb{R}^4$

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

es tal que $\overline{V\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)}$ tiene infinitas componentes conexas (puesto que su proyección en la primera componente es $\mathbb{Z}$). Aritméticamente hablando $\mathbb{Z}\left[\frac{1}{2}\right]$ es muy diferente a $\mathbb{Q}$. En general, por resultados de J. Robinson, si P es un conjunto finito de primos tenemos que $\mathbb{Z}$ es diofantino en $\mathbb{Z}[P^{-1}]$. En 2003, B. Ponnen [7] dió los primeros ejemplos con P infinito. Su teorema no usa la aritmética de las formas cuadráticas: ¡usa curvas elípticas! Su resultado dice:

Existe un conjunto infinito, recursivo de números primos P y una curva elíptica V definida sobre $\mathbb{Z}[P^{-1}]$ tal que $\overline{V(\mathbb{Z}[P^{-1}])} \subset V(\mathbb{R})$ tiene infinitos componentes conexas, y el décimo problema de Hilbert *sobre $\mathbb{Z}[P^{-1}]$ es insoluble.*

Poonen muestra que P es grande en cierto sentido técnico (pero P no es todo el conjunto de primos). Parte del problema radica en que P debe ser recursivo para que el anillo $\mathbb{Z}[P^{-1}]$ resulte recursivo (sino el problema de Hilbert no tendría sentido). También note que Poonen no demuestra que $\mathbb{Z}$ es diofantino en $\mathbb{Z}[P^{-1}]$ sólo que admite a $\mathbb{Z}$ como modelo diofantino.

4. **Curvas elípticas**

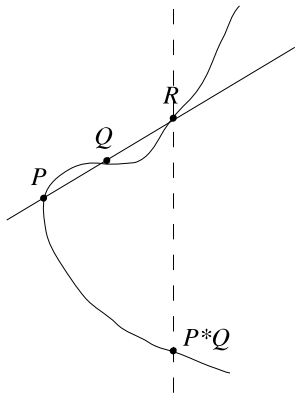
La referencia básica que usé es el libro de Silverman [10]. En esta sección explicamos lo mínimo necesario para la aplicación al teorema de R. Robinson.

Definición 4.1.

1) Una curva elíptica E sobre $\mathbb{Q}$ es una curva en $\mathbb{R}^2$ definida por
$$E : y^2 - (ax^3 + bx^2 + c + d) = 0$$
con $a, b, c, d \in \mathbb{Q}$ tal que la cúbica $ax^3 + bx^2 + cx + d$ no tiene raíces múltiples en $\mathbb{C}$.
2) $E(\mathbb{Q}) := \{(r, s) \in \mathbb{Q}^2 | s^2 = ar^3 + br^2 + cr + d\} \cup \{\infty\}$. Aquí ∞ es un símbolo que representa el punto al "infinito".

4.2. **La ley de grupo sobre $E(\mathbb{Q})$.** Lo útil de estas cúbicas es que hay una operación binaria $*$ sobre $E(\mathbb{Q})$ que da la estructura de grupo abeliano a $E(\mathbb{Q})$:

i) ∞ es el elemento neutro.
ii) Si $P, Q \in E(\mathbb{Q})$, $P \neq \infty$, $Q \neq \infty$, $P \neq Q$ y si $R(x, y)$ es el tercer punto de intersección de la curva elíptica con la línea ℓ que une P a Q, ponemos $P * Q = (x, -y)$.
Evidentemente $P * Q \in E(\mathbb{Q})$.
iii) Si $P = Q(\neq \infty)$, usamos la tangente a P.
iv) Si $P \in E(\mathbb{Q})$, $P \neq \infty$ y $P = (x, y)$ entonces $-P = (x, -y) \in E(\mathbb{Q})$.



4.3. **"$*$"es algebraica.** La operación $*$ es algebraica, es decir las coordenadas de $P * Q$ vienen dadas por funciones racionales (con coeficientes en $\mathbb{Q}$) en las coordenadas de P y Q. Veamos esto en detalle. Sean $P, Q \neq \infty$, $P(x_1, y_1)$ y $Q(x_2, y_2)$.

a) Supongamos $x_1 \neq x_2$. La linea que une a P a Q tiene ecuaciones

$$y = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x - x_1) + y_1 \,. \tag{7}$$

Para encontrar los puntos de intersección entre la curva y la linea sustituimos el valor de y en (7) en la ecuación. Esto produce una cúbica (con coeficientes en $\mathbb{Q}$) de la cual sabemos que x_1 y x_2 son dos raíces racionales. Tenemos pues

$$qx^3 + rx^2 + sx + t = q(x - x_1)(x - x_2)(x - x_3).$$

Se deduce que $x_3 \in \mathbb{Q}$. Sustituyendo x_3 en (7) obtenemos un valor $y = y_0$.

Definimos $y_3 = y_0$.

Entonces $P * Q = (x_3, y_3)$.

Haciendo todas las cuentas se obtiene

$$\begin{aligned} x_3 &= \frac{1}{a}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - \frac{b}{a} - x_1 - x_2 \\ y_3 &= -\left(\frac{y_2 - y_1}{x_2 - x_1}\right)x_3 + \frac{y_2 x_1 - y_1 x_2}{x_2 - x_1} \,. \end{aligned}$$

b) Suponga $x_1 = x_2$. Aquí hay dos subcasos.

Si $y_1 = y_2$ entonces $P * Q = \infty$. Este caso inlcuye el caso $y_1 = 0$.

Si $y_1 \neq -y$, entonces $y_1 \neq 0$ y tenemos $P = Q$. Hay que usar la tangente en P y obtenemos

$$y = \left(\frac{3ax_1^2 + 2bx_1 + c}{2y_1}\right)(x - x_1) + y_1\,. \tag{8}$$

Haciendo lo mismo que en el caso a) obtenemos una cúbica con coeficientes en $\mathbb{Q}$ y con $x = x_1$ como raíz doble:

$$qx^3 + rx^2 + sx + t = q(x - x_1)^2(x - x_3)\,.$$

Otra vez, $x_3 \in \mathbb{Q}$. Substituyendo en (8) obtenemos un valor $y = y_0$. Defina $y_3 = -y_0$. Entonces $P * Q = 2P = (x_3, y_3)$. Haciendo todas las cuentas tenemos:

$$\begin{aligned} x_3 &= \frac{1}{4ay_1^2}(a^2x_1^4 - 2acx_1^2 - 8adx_1 + c^2 - 4bd) \\ y_3 &= \frac{1}{8ay_1^3}\Big(a^3 + x_1^6 + 2a^2bx_1^5 + 5a^2cx_1^4 + 20a^2dx_1^3 \\ &\quad +(20dab - 5ac^2)x_1^2 + (8b^2d - 2bc^2 - 4acd)x_1 \\ &\quad +(4bcd - 8ad^2 - c^3)\Big)\,. \end{aligned}$$

Es fácil ver que $P * Q = Q * P$; la asociatividad es más complicada. En principio se puede verificar usando las formulas. Existen principios geométricos que ofrecen demostraciones más cortas y conceptuales (ver el libro de Silvermann). El hecho es que $*$ es asociativa. Por lo tanto $E(\mathbb{Q})$ es un grupo abeliano. Note lo siguiente: para cada campo $F \subset \mathbb{C}$ podemos considerar las soluciones a E con coordenadas en F. Por lo que acabamos de hacer, la operación $*$ viene dada por funciones racionales en las coordenadas pero estas funciones racionales tienen coeficientes en $\mathbb{Q}$. Por lo tanto

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

es un grupo (abeliano) también. En particular $E(\mathbb{R})$ es un grupo abeliano.

4.4. **La curva $y^2 = x^3 - 4$.** Esta curva es la que usa R. Robinson. Usando las fórmulas en 4.3 con $a = 1$, $b = c = 0$ y $d = -4$ tenemos:

a) Si $P = (x_1, y_1)$ y $Q(x_2, y_2)$ entonces

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

y si $x_1 \neq x_2$

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

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

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

Los únicos puntos $Q \in E(\mathbb{Q})$ con coordenadas en $\mathbb{Z}$ son $(2, \pm 2)$ y $(5, \pm 11)$.

Esto lo demostró FERMAT. Para el argumento de R. ROBINSON necesitamos el siguiente resultado:

Proposición 4.5. *$E(\mathbb{Q})$ es infinito y denso en $E(\mathbb{R})$.*

Demostración. Sea $r \neq 0$ $r \in \mathbb{Q}$ $r = \dfrac{m}{n}, (m, n) = 1$. Definimos el tamaño $t(r)$ como:

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

Si $P \in E(\mathbb{Q})$ entonces ponemos $t(P) = t(x)$ donde $P = (x, y)$ y $t(\infty) = 0$. Para ciertos puntos $P \in E(\mathbb{Q})$ vamos a mostrar que el tamaño de $2P$ es mucho más grande que el tamaño de P. Supongamos que $P = (\dfrac{m}{n}, y)$ con $m, n \in \mathbb{Z}$ $(m, n) = 1$. La coordenada x de $2P$ es igual a $\dfrac{(m^3 + 32n^3)m}{4n(m^3 - 4n^3)}$.

Supongamos ahora que elegimos P tal que m es impar. Entonces se sigue que $(4n, m(m^3 + 32n^3)) = 1$. Luego cualquier cancelación entre el numerador y el denominador de la coordenada x de $2P$ no afecta al factor 4. Entonces $t(2P) \geq 4$ y el numerador de la primera coordenada de $2P$ sigue siendo impar. Claramente, por inducción, tenemos:

$$t(2^k P) \geq 4^k \quad \text{para} \quad k \geq 1$$

Esto implica que la sucesión de puntos $P, 2P, 4P, \ldots$ tiene infinitos puntos diferentes pues de lo contrario la sucesión de números enteros $t(P), t(2P), t(4P), \ldots$ estaría acotada lo cual no es posible. Sólo falta elegir a P. Tomemos $P = (5, 11)$. No sólo tenemos que $E(\mathbb{Q})$ es infinito sino también hemos probado que el subgrupo generado por $(2, 2)$ es isomorfo a $\mathbb{Z}$. Para la segunda parte observe lo siguiente: el grupo abeliano $E(\mathbb{R})$ es topológicamente isomorfo a $\mathbb{R}/\mathbb{Z}$. Aquí el punto al "infinito" ∞ corresponde a $0 \in \mathbb{R}/\mathbb{Z}$. La imagen del subgrupo $\langle (2, 2) \rangle$ dentro de $\mathbb{R}/\mathbb{Z}$ es infinita luego a $(2, 2)$ le corresponde un número irracional γ en $\mathbb{R}/\mathbb{Z}$. El grupo generado por γ es por lo tanto denso; luego $\langle (2, 2) \rangle$ es denso en $E(\mathbb{R})$. Como $\langle (2, 2) \rangle \subseteq E(\mathbb{Q})$ esto implica lo que queríamos. ☑

Necesitamos un último resultado sobre E. Sean $f(t)$, $g(t)$ son funciones racionales con coeficientes en $\mathbb{Q}$. Si

$$f(t)^2 = g(t)^3 - 4$$

entonces f y $g \in \mathbb{Q}$.

La demostración de este resultado se encuentra en los últimos ejercicios de estas notas. Le agradezco a el alumno D. Gómez haber notado un error en el argumento original que presenté en Bogotá.

Hasta ahora no existe un algoritmo que decida, dada una curva elíptica sobre $\mathbb{Q}$, si ésta posee un punto P con coordenadas racionales (el punto ∞ no cuenta como punto con coordenadas racionales).

5. **Teorías elementales**

Necesitamos algunas nociones y resultados de la lógica matemática. Hemos estado considerando a $\mathbb{Z}$ y $\mathbb{Q}$ como estructuras algebraícas: queremos saber que ecuaciones tiene solución y cuales no. Generalizando esto podemos estudiar sus propiedades algebraicas. ¿Qué es una propiedad algebraica? Para nosotros una propiedad algebraica es una que se puede escribir en términos de la suma, resta, multiplicación, variables y las constantes 0 y 1 junto con los conectivos lógicos: $=, \wedge\vee, \neg, \rightarrow, \exists, \forall$. Los cuantificadores $\exists$ y $\forall$ ("existe" y "paratodo") sólo cuantifican sobre elementos; no cuantifican sobre subconjuntos o funciones. Si una propiedad algebraica se puede formular de la manera pedida anteriormente, la llamamos elemental. Por ejemplo, la propiedad que dice que todo polinomio de grado dos tiene una raiz, es elemental:

$$\varphi \equiv \forall a, b, c \Big((a \neq 0) \rightarrow \exists x (ax^2 + bx + c = 0) \Big).$$

La propiedad de inducción de $\mathbb{N}$ no es elemental.

Para estructuras como $\mathbb{N}, \mathbb{Z}$ o $\mathbb{Q}$ (o en general un campo K) definimos la teoría de la estructura $T(\mathbb{N}), T(\mathbb{Z})$, etc, como el conjunto de propiedades elementales verdaderas en la estructura. Por ejemplo, para φ arriba, $\varphi \notin T(\mathbb{Q})$ pero $\varphi \in T(\mathbb{C})$.

La teoría $T(K)$ contiene gran cantidad de la aritmética de K. El teorema de Lagrange:

$$\forall x \exists a, b, c, d (x = a^2 + b^2 + c^2 + d^2)$$

pertenece a $T(\mathbb{N})$.

Como el conjunto de propiedades elementales es reconocible por un computador tiene sentido la siguiente pregunta. Dada una estructura K como las que venimos considerando, ¿Existe un algoritmo que, para cada propiedad elemental φ, decida si $\varphi \in T(K)$?

Si el algoritmo existe la teoría se llama *soluble*. De lo contrario *insoluble*.

Teorema 5.1. [Gödel, Church, Rosser, 1930–40] *Las teorías $T(\mathbb{N})$, $T(\mathbb{N}^+)$ y $T(\mathbb{Z})$ son insolubles.*

Aquí $\mathbb{N}^+$ es el conjunto de números naturales positivos.

Este teorema se debe contrastar con los siguientes resultados anteriores: Presburger había demostrado que la teoría aditiva de $\mathbb{Z}$, donde sólo se usa

la suma, es soluble y SKOLEM había demostrado que la teroía multiplicativa, donde sólo se usa la multiplicación, también es soluble.

En su tesis doctoral de 1949, JULIA ROBINSON demostró (entre otras cosas) que $T(\mathbb{Q})$ es insoluble. Para explicarlo brevemente necesitamos la siguiente

Definición 5.2. Para una estructura K decimos que un subconjunto $S \subset K^n$ es *definible* si existe una propiedad algebraica $\varphi(x_1, \ldots, x_n)$ tal que para $(a_1, \ldots, a_n) \in K^n$ vale: $(a_1, \ldots, a_n) \in S \leftrightarrow \varphi(a_1, \ldots, a_n)$ es verdadera en K.

Cada conjunto diofantino es definible. En general, hay conjuntos definibles que no son diofantinos.

Ejemplos:

a) En $\mathbb{N}$ el conjunto de números primos P es definible:

$$n \in P \leftrightarrow (n^2 \neq n) \wedge (\forall x(x|n \rightarrow ((x = 1) \vee (x = n)))$$

La expresión $x|n$ debe ser expresada en términos de sumas y productos. Pero esto es fácil: $x|n \leftrightarrow \exists z(n = z \cdot x)$. Es un hecho no trivial que P es un subconjunto diofantino!

b) En $\mathbb{N}, \mathbb{Z}$ o $\mathbb{Q}$ el orden es definible:

$$x \geq y \leftrightarrow \exists z_1, \ldots, z_4 : x - y = \sum_{i=1}^{4} z_i^2.$$

c) En $\mathbb{R}$, $x \geq y \leftrightarrow \exists z(x - y = z^2)$

Sobre campos hay una interpretación geometría de los subconjuntos definibles. Lo único que se puede construir con $+, -, \cdot, 0, 1$ y variables son polinomios con coeficientes en $\mathbb{Z}$.

Luego, con "=" tenemos ecuaciones. Note ahora las equivalencias:

(i) $u \neq 0 \leftrightarrow \exists \omega(u\omega - 1 = 0)$,
(ii) $(u = 0) \wedge (v = 0) \leftrightarrow \forall x, y(ux = vy)$;
(iii) $(u = 0) \vee (v = 0) \leftrightarrow u \cdot v = 0$,
(iv) $\forall x \leftrightarrow \neg\exists x\neg$; $\neg\forall x \leftrightarrow \exists x\neg$

Por lógica general se pueden sacar todos los cuantificadores al frente luego cada $\varphi(x_1, \ldots, x_n)$ tiene la forma $Q_1\omega_1 Q_2\omega_2 \cdots Q_m\omega_m(F(\vec{x}, \vec{\omega}) = 0)$ donde $Q_i = \forall, \exists$ y $F \in \mathbb{Z}[\vec{x}, \vec{\omega}]$.

Por (iv) vemos que un conjunto definible $S \subset K$ se obtiene de un conjunto algebraico por medio de proyecciones y complementaciones.

El gran resultado de J. ROBINSON [8] es

Teorema 5.3. *$\mathbb{Z}$ es definible en $\mathbb{Q}$.*

No es el objetivo de este curso presentar su demostración. Su prueba se basa en la artimética de las formas cuadráticas en tres variables.

Corolario 3. *$T(\mathbb{Q})$ es insoluble.*

La demostración de esto es parecida a la del corolario en 2.4.

Hasta ahora no existe otra demostración para la insolubilidad de $\mathbb{Q}$. En [12] hay un intento para reducir la complejidad de la definición anterior. Este intento se basa en el uso de curva elípticas. Para resumir: sabemos que $\mathbb{Z}$ se obtiene por proyecciones y complementaciones de algún conjunto algebraico en $\mathbb{Q}^n$, para algún n. No sabemos si se pueden usar sólo proyecciones.

El corolario 3 implica que cada vez que $\mathbb{Q}$ sea definible en un campo K, la teoría $T(K)$ es insoluble. Esto es lo que hace R. Robinson para $K = \mathbb{Q}(t)$. El caso general, donde $K = F(t)$ con F ordenable, procede de manera muy diferente.

Aquí, él no logra definir a $\mathbb{Q}$ dentro de $F(t)$ pero construye una copia de la estructura $\widetilde{\mathbb{N}} = (\mathbb{N}^+, +, |)$ donde $\mathbb{N}^+$ son los naturales positivos, $+$ es la suma y $|$ la división. Esto es suficiente pues tenemos el

Lema 5. *La teoría $T(\widetilde{\mathbb{N}})$ es insoluble.*

Demostración. Aquí $\widetilde{\mathbb{N}}$ es vista como una estructura con la suma y la división. En vista del teorema 5.1 basta probar que la multiplicación de naturales positivos es definible en términos de $+$, $|$.

Vale la pena notar que J. Robinson en su tesis mostró como definir la suma y producto de naturales positivos usando solamente la función sucesor $S(x) = x + 1$ y la división.

Dejamos como ejercicio verificar las siguientes equivalencias dadas por Tarski para naturales positivos,

a) $n = k(k+1) \leftrightarrow \forall m(n|m \leftrightarrow k|m \wedge k+1|m)$
b) $n = k\ell \leftrightarrow (k+\ell)(k+\ell+1) = k(k+1) + \ell(\ell+1) + n + n$

En estricto rigor el número 1 se debe eliminar del lado derecho de a):

$r = 1 \leftrightarrow \forall\omega(r|\omega)$. Entonces el lado derecho de a) queda como $\varphi(n,k) \equiv \forall m(n|m \leftrightarrow k|m \wedge \forall r(\forall\omega(r|\omega) \rightarrow k + r|m))$. (Entonces $\varphi(n,k) \leftrightarrow n = k(k+1)$). ☑

6. **Teoremas de R. Robinson**

Teorema 6.1. [R. Robinson 1950]. *La teoría $T(\mathbb{Q}(t))$ es insoluble*

Demostración. Vamos a definir a $\mathbb{Q}$ artiméticamente en $\mathbb{Q}(t)$. Para $x, y \in \mathbb{Q}(t)$ definimos $x \geq y \leftrightarrow \exists\omega_1, \omega_2, \omega_3, \omega_4 \in \mathbb{Q}(t)$ tal que $x - y = \omega_1^2 + \omega_2^2 + \omega_3^2 + \omega_4^2$. Observe que si $x, y \in \mathbb{Q}$ entonces $x \geq y$ coincide con el orden en $\mathbb{Q}$.

También definimos Ord(y) para $y \in \mathbb{Q}(t)$ com $\exists x \in \mathbb{Q}(t)(y^2 = x^3 - 4)$. Por lo que vimos en la sección 3, si Ord(y) es cierto entonces $y \in \mathbb{Q}$. El conjunto $\{y : Ord(y)\}$ es un subconjunto denso de $\mathbb{Q}$.

Sea $r \in \mathbb{Q}(t)$. Definimos

$$\text{Con}(r) \leftrightarrow \forall y(Ord(y) \Rightarrow (r - y \geq 0) \vee (y - r \geq 0))$$

Afirmación:$Con(r) \leftrightarrow r \in \mathbb{Q}$.

Demostración. "$\Leftarrow$": claro.

"$\Rightarrow$": Suponga que no: $r \in \mathbb{Q}(t) - \mathbb{Q}$. Entonces r es una función racional no constante. Sabemos como es la gráfica de este tipo de funciones. Debe haber un intervalo (α, β) propiamente contenido en la imagen $r(\mathbb{R})$. Para s racional cualquiera en (α, β) $r - s \geq 0$ y $s - r \geq 0$ son falsas. Por la densidad de Ord en $\mathbb{Q}$ podemos elegir $s \in \mathbb{Q}$ con Ord (s). Luego no vale Con(r). ☑

La idea es muy simple y elegante. El grupo $E(\mathbb{Q}(t))$ es igual a $E(\mathbb{Q})$. Las segundas coordenadas de puntos en la curva definen un subconjunto denso de $\mathbb{Q}$. Y si una función racional es comparable con cada uno de los números en este conjunto entonces debe ser constante. En la decada de los 50 y principios de los 60 varias personas extendieron este resultado. Entre ellos están J. ROBINSON, A. TARSKI y A. MALCEV. La idea predominante era que el teorema debería ser cierto para campos K ordenables. El argumento de R. ROBINSON tenía que ser modificado pues, por ejemplo, directamente no servía para demostrar la insolubilidad del campo $\mathbb{R}(t)$. Esto es claro porque para $g \in \mathbb{R}(t)$, Ord$(g) \Leftrightarrow g \in \mathbb{R}$; pero el campo $\mathbb{R}$ tiene teoría soluble. Se logró demostrar (dejando de lado a las curvas elípticas) el teorema cuando K es real cerrado, es decir K elementalmente equivalente a $\mathbb{R}$. De hecho MALCEV conjeturó que $K(t)$ tiene teoría insoluble para cualquier campo K. Esta conjetura se ha demostrado en muchos casos ¡pero está sin resolver cuando $K = \mathbb{C}$!

PHEIDAS [6] ha logrado mostrar que $F(t)$ tiene teoría insoluble si F es un campo de característica $p \geq 5$. Su demostración usa curvas elípticas. Un buen problema para una tesis de maestría consiste en extender su resultado a características 2 y 3.

Volviendo al caso en donde K es ordenable, fué en 1964 que R. ROBINSON logró demostrar la insolubilidad de $K(t)$. Su demostración usa su idea de usar la curva elíptica $y^2 = x^3 - 4$ junto con ideas de las demostraciones de J. ROBINSON, TARSKI y MALCEV para el caso en que K es real cerrado.

Teorema 6.2. [R. ROBINSON [9]]. *Sea K ordenable. Entonces $K(t)$ tiene teoría insoluble.*

La idea de la demostración es la siguiente. La curva elíptica $y^2 = x^3 - 4$ tiene una copia de $\mathbb{Z}$, a saber el grupo $\langle(2, 2)\rangle$. Este grupo forma parte de $E(K(t))$. Escribiendo $n(2, 2) = (x_n, y_n)$ para $n \geq 1$ (donde $n(2, 2)$ es la suma $*$ en E de $(2, 2)$ n–veces), ROBINSON logra definir una división D sobre las segundas coordenadas que satisface $y_n D y_m \Leftrightarrow n|m$ (sólo para $n, m \geq 1$). La suma $y_n * y_m$ es la suma sobre la curva. Finalmente se verá que la estructura $(\{y_n : n \geq 1\}, *, D)$ es isomorfa a la estructura $\widetilde{\mathbb{N}}$ (de 5.4).

Comencemos con la suma.

Definición 6.3. Para $b, d, y \in K(t)$ definimos $y = b * d \Leftrightarrow \exists a, c, m, x \in K(t)$ tales que

$$\begin{aligned}(b^2 = a^3 - 4) \wedge (d^2 = c^3 - 4)\\ \wedge \quad ((c-a)m = d - b) \wedge (d = b \rightarrow 2bm = 3a^2)\\ \wedge \quad (x = m^2 - a - c) \wedge (y = -mx + ma - b)\end{aligned}$$

Nota: Lo que la fórmula de arriba dice es que y es la segunda coordenada del punto $(a, b) * (c, d)$ sobre $E : y^2 = x^3 - 4$ (vea las fórmulas de la sección 4). Si $y = b * d$ es verdad, entonces los puntos (a, b) y (c, d) no están en línea vertical (pues si lo estuvieran, m que es la pendiente, no existiría). Luego $b \neq -d$. Si $(a, b), (c, d) \in \mathbb{Q}^2$ y vale $b * d = y$ entonces $(x, y) \in \mathbb{Q}^2$ y vale $b + d = y$ entonces $(x, y) \in \mathbb{Q}^2$. Recondando que hemos definido x_n, y_n como $n(2, 2) = (x_n, y_n)$ tenemos

Lema 6. $\forall n, m \geq 1\ y_n * y_m = y_{n+m}$.

Demostración. Es claro pues $y_n * y_m$ es la segunda coordenada del punto

$$n(2, 2) * m(2, 2) = (n + m)(2, 2) \qquad \boxtimes$$

El siguiente paso es el definir el subconjunto $\{y_n : n \geq 1\} \subset \mathbb{Q} \subset K(t)$ y luego una división D tal que $y_n D y_m \Leftrightarrow n|m$.

Aquí Robinson se inspiró en los trabajos de Malcev, Tarski y J. Robinson. Malcev fué el primero en representar a $\mathbb{N}$ como el conjunto de raíces de una función racional.

Para $x \in K(t), x \in \mathbb{N}^+ \Leftrightarrow$

$$\exists f \in K(t)(f(1) = 0 \wedge \forall \omega \in K((\omega \neq x \wedge f(\omega) = 0) \rightarrow f(\omega + 1) = 0)).$$

La idea es que para $x = n$ tomamos $f(t) = (x - 1)(x - 2) \cdots (x - n)$. Por otro lado, si el lado derecho es verdad y $x \neq n$ para toda $n \geq 1$ obtenemos una contradicción. Empezando con $f(1) = 0$ y $x \neq 1$ obtenemos que $f(2) = 0$. Por inducción $f(n) = 0 \forall n \geq 1$. Esto no puede pasar para una función racional pues $f(x) = 0$ sólo tiene un número finito de soluciones en K. Obviamente esta expresión no es elemental. El cuantificador $\forall \omega \in K$ se puede areglar fácilmente usando la fórmula $\forall \omega(\mathrm{Ord}\omega \wedge \cdots$ donde $\mathrm{Ord}(\omega) \equiv \exists s \in K(t)(\omega^2 = s^3 - 4)$. El problema grave es como expresar la afirmación "$f(\omega) = 0$". En general (es decir para K un campo cualquiera) no se sabe como hacer. Cuando $K = \mathbb{R}$ (o en general cuando K es real cerrado) Malcev uso el hecho que el orden del campo $\mathbb{R}(t)$ es definible: para $f, g \in \mathbb{R}(t)$ vale

$$f \leq g \Leftrightarrow \exists \omega, s \in \mathbb{R}(t) : g - f = \omega^2 + s^2.$$

Si quiero afirmar que $f(5) = 0$, por ejemplo, lo puedo hacer así:

$$f^2 \leq (t - 5)^2$$

Si bien esto implica que $f(5) = 0$, no estamos del otro lado pues tenemos un símbolo que no se puede usar: la variable t. Además, $f(5) = 0$ sólo implica que $(t-5)$ es un factor del numerador pero no necesariamente vale la desigualdad (ni localmente y menos globalmente). Otro obstaculo es el uso del orden. Si K es ordenable también se puede ordenar $K(t)$. Pero hay diferentes órdenes y los hay que no son definibles mediante suma de cuadrados. MALCEV consiguió resolver estos problemas para algunos K pero la idea clave que usa R. ROBINSON viene de una construcción de J. ROBINSON.

6.4. **Construcción de J. Robinson.** Si $r_1, r_2, \ldots, r_n \in \mathbb{Q}$, existe $f \in \mathbb{Q}(t)$ tal que

(i) $f^2(t) \leq (t - r_i)^2 \quad \forall t \in \mathbb{Q}$
(ii) $f(t) = 0 \Leftrightarrow t = r_i$.

Dejamos la construcción de f para los ejercicios.

El problema del orden se resuelve de la siguiente forma: lo único que vamos a comparar son funciones f, g que tendrán coeficientes en $\mathbb{Q}$ y entonces podemos usar el siguiente teorema de HILBERT: Si $f, g \in \mathbb{Q}(t)$ entonces

$$\begin{aligned} f \geq g &\Leftrightarrow \exists r_1, r_2, \ldots, r_8 \in \mathbb{Q}(t) : \\ (f - g) &= \sum_{i=1}^{8} r_i^2 \end{aligned}$$

Pensando en que y_n es "el número n" definimos

$$z|_t y \Leftrightarrow \exists g \Big[g \neq 0 \wedge g^2 \leq (t-2)^2 \wedge$$
$$\forall z \Big[(\mathrm{Ord}(z) \wedge z \neq y \wedge g^2 \leq (t-z)^2) \rightarrow \exists z' (z * 2 = z' \wedge g^2 \leq (t - z')^2) \Big]$$

Observe que $*$ es definible en términos de $+, -, \cdot$, del campo $K(t)$. Hemos usado la variable t: por eso usamos el subíndice. El símbolo $\leq$ se elimina vía la suma de ocho cuadrados.

Lema 7.
a) $2|_t y \Leftrightarrow y = y_n$.
b) $\forall n, m \geq 1 \; y_n|_t y_m \Leftrightarrow n|m$

Demostración.

a) "$\Rightarrow$": Suponga $y \neq y_n \forall n \geq 1$. Como $g^2 \leq (t-2)^2$ tenemos $g(2) = 0$. Sabemos que vale $\mathrm{Ord}(2), y \neq y_1 = 2$ luego $y_2 = 2 * 2$ satisface $g^2 \leq (t - y_2)^2$. Esto implica $g(y_2) = 0$. Inductivamente demostramos que $g(y_n) = 0 \forall n \geq 1$. ¡Esto es imposible para una función racional!
"$\Leftarrow$": Sea y_n dado. Tomemos $r_1 = 2$, $r_2 = y_2, \ldots, r_n = y_n$. Note que estos números son racionales. Sea $g \in \mathbb{Q}(t)$ la función de la construcción

en 6.5. Claramente vale $2|_t y_n$ puesto que $g \in \mathbb{Q}(t)$ y el orden en este campo satisface el teorema de Hilbert.

b) Lo que hay que demostrar aquí e0s lo siguiente: $y_n|_t y_m \Leftrightarrow y_m = \ell * y_n$ para algún $\ell \geq 1$ (es decir y_m es y_n sumado ℓ veces).

La demostración es como la de a) usando 6.4. ☑

El siguiente resultado es clave para la eliminación de t.

Sublema: *Si $(a, b) \in \mathbb{Q}^2$ y $b^2 = a^3 - 4$, entonces $b|_t d \Leftrightarrow d = n * b$ para algún $n \geq 1$.*

Demostración. Es parecido a lo anterior. Si $b|_t d$ entonces, si $d \neq n * b \; \forall n \geq 1$, concluímos que todos los números $n * b$ (que son infinitos puesto que $n * (a, b) \neq \infty$) son raíces de una función racional. Esto es imposible. En la otra dirección podemos usar la construcción de J. Robinson puesto que $m * b \in \mathbb{Q}$ para $1 \leq m \leq n$. ☑

El Lema 7 se podría haber deducido del sublema. Lo importante es que $b|_t d$ tenga el significado que queremos cuando $b, d \in \{y_n : n \geq 1\}$. Finalmente definimos D.

Para $x, y \in K(t)$ definimos xDy si y sólo si:

$$\forall \omega \left(\left(x|_\omega x \wedge \forall z, z' \left[(x|_\omega z \wedge z' = x * z) \rightarrow x|_\omega z' \right] \right) \rightarrow x|_\omega y \right).$$

Proposición 6.5. *Si $b^2 = a^3 - 4$, $a, b \in \mathbb{Q}$ tenemos $bDd \Leftrightarrow$ existe $n \geq 1$ con $d = n * b$.*

Demostración. Si $d = n * b$ entonces claramente bDd.

Supongamos ahora que bDd. Tomemos $\omega = t$. Entonces $b|_t b$ (podemos usar $g(t) = ((t - b)^2)$. Suponiendo que $b|_t \omega$ y que $\omega' = b * \omega$ podemos concluir que $b|_t \omega'$ por el sublema (en una dirección da que $\omega = n * b$ y entonces $\omega' = b * (n * b) = (n + 1) * b$; en la otra dirección esto da $b|_t \omega'$).

Concluímos que debe valer $b|_t d$. Otra vez por el sublema tenemos $d = n * b$. ☑

Tenemos entonces

Proposición 6.6.

$$(\{y_n : n \geq 1\}, *, D) \cong (\mathbb{N}^+, +, |)$$

Demostración. La correspondencia $y_n \rightarrow n$ da el isomorfismo en vista de 6 y del hecho que $y_n D y_m \Leftrightarrow y_m = \ell * y_n$ (por 6.5) $= y_{\ell_n}$ (por 6). Luego $m = \ell n$ es decir $n|m$. ☑

Podemos completar la demostración de 6.2: $K(t)$ tiene de manera definible una estructura isomorfa a $\widetilde{\mathbb{N}}$. Como $T(\widetilde{\mathbb{N}})$ es insoluble (5) esto implica que $T(K)$ es insoluble.

7. ¿Qué sigue?

En 1970 se conoció que $H10(\mathbb{Z})$ es insoluble. A partir de entonces cobró importancia saber si lo mismo ocurría con otros anillos o campos. Obviamente que el campo $\mathbb{Q}$ es el más destacado. En 1980 DENEF logró demostrar que $H10(K(t))$ con K ordenable es insoluble. Su idea es la de usar no sólo la aritmética de curvas elípticas sino el anillo de endomorfismos de las curva. Esta es la gran nueva idea que PHEIDAS a explotado muchísimo. Para quienes les haya interesado este asunto el paso que sigue es el de estudiar [2], [6] y los artículos en [5]. Finalmente menciono que en [11] hay un uso de las curvas elípticas basado en ideas distintas a las que hemos visto aquí. Sería interesante poder replicar la construcción de R. ROBINSON directamente sobre $\mathbb{Q}$ aún usando cuantificadores universales. Esto daría una demostración nueva de la insolubilidad de $T(\mathbb{Q})$.

Ejercicios

(1) Demuestre que la ecuación

$$(2x+3)(5x+7)=0$$

tiene solución en $\mathbb{R}$ y $\mod(p^n)$ para cada primo p y $n \geq 1$.
Ayuda: Use la siguiente versión del Lema de HENSEL: Si $f \in \mathbb{Z}[x]$ y $a \in \mathbb{Z}$ satisface $f(a) \equiv 0 \mod (p)$ y $f'(a) \not\equiv 0 \mod (p)$ entonces para cada $n \geq 1$ la congruencia $f \equiv 0 \mod(p^n)$ tiene una solución a_n.

(2) Complete la tabla 2.7

(3) Pruebe que la ecuación $y^2 = x^3 + 7$ no tiene soluciones enteras.
Solución: x no puede ser par pues $y^2 \equiv 7 \mod (8)$ no tiene soluciones (ver la tabla 2.7). Entonces

$$y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4).$$

Como x es impar tenemos que

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

Como productos de números de la forma $4n+1$ son de ésta forma se sigue que $x^2 - 2x + 4$ tiene un divisor primo $p \equiv 3 \mod (4)$. Luego la congruencia $y^2 \equiv -1 \mod (p)$ tiene solución. Esto es imposible pues -1 es sólo residuo cuadrático de primos congruentes a uno mod (4). La solución es de V. LEBESGUE 1869.

¿Tiene la ecuación $y^2 = x^3 + 7$ soluciones en $\mathbb{Q}$?

(4) Pruebe que la ecuación

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \mod(p^n)$$

tiene solución para todo primo p y entero $n \geq 1$.

(5) Usando el teorema de LAGRANGE demuestre que para $r \in \mathbb{Q}$ vale

$$r \geq 0 \Leftrightarrow \exists a, b, c, d \in \mathbb{Q} : r = a^2 + b^2 + c^2 + d^2$$

(6) Escriba el siguiente teorema de Fermat como una propiedad elemental de $\mathbb{N}$: Todo primo de la forma $4n+1$ es suma de dos cuadrados.

(7) Muestre que el conjunto de potencias de 2 es definible en $\mathbb{N}$.
Solución: Sea $S = \{2^n : n \geq 0\}$. Entonces

$$x \in S^c \Leftrightarrow \exists a, b(b \neq 0 \wedge x = a(2b+1))$$

Luego $x \in S \Leftrightarrow \neg\exists a, b(b \neq 0 \wedge x = a(2b+1))$.

Observe que S^c es diofantino:

$$b \neq 0 \Leftrightarrow \exists\omega(b = \omega + 1)$$

De hecho S también es diofantino pero esto no es fácil de probar.

(8) Verifique las ecuaciones que dan $P * Q$ algebraicamente.

(9) Demuestre: si $f, g \in \mathbb{R}(t)$ entonces

$$f \leq g \Leftrightarrow \exists u, \omega \in \mathbb{R}(t) : g - f = u^2 + \omega^2$$

Solución: Podemos suponer que $g-f$ es un polinomio. Pues si $g-f = \dfrac{h}{r}$ con $h, r \in \mathbb{R}[t]$ tenemos $\dfrac{h}{r} = \dfrac{h \cdot r}{r^2}$ lo cual implica $h \cdot r \geq 0$. Factorizando $g - f$ en $\mathbb{R}[t]$ tenemos

$$g - f = a^2 \prod_j (t - c_j)^2 \cdot \prod_\ell (b_\ell^2 + (t - a_\ell)^2)$$

Usamos ahora la famosa identidad:

$$(\alpha^2 + \beta^2)(\gamma^2 + \delta^2) = (\alpha\gamma - \beta\delta)^2 + (\alpha\delta + \beta\gamma)^2$$

Esto muestra que el segundo producto (sobre ℓ) es suma de dos cuadrados.

(10) (R. Robinson).
En $\mathbb{Z}$ demuestre:
i) $x \geq 0 \leftrightarrow \exists y, z\omega(4x + 1 = y^2 + z^2 + \omega^2)$
ii) $x \geq 0 \wedge \neg\exists y(x = y^2) \Leftrightarrow \exists y\exists z(y^2 = 1 + xz^2 \wedge y^3 \neq y)$
iii) $x \geq 0 \leftrightarrow \exists y\exists z[(x = y^2) \vee (y^2 = 1 + xz^2 \wedge y^3 \neq y)]$.
Solución: iii) se deduce de ii).

Para ii) observe lo siguiente. La ecuación de Pell $x^2 - ay^2 = 1$ tiene infinitas soluciones si a es positivo y diferente a un cuadrado. (En clase vimos esto para $a = 2$). Cuando $a = b^2$ entonces $x^2 - b^2y = (x - by)(x + by) = 1$. Luego $x = \pm 1$. Y si $a < 0$ entonces $x^2 \leq 1$. Esto prueba ii).

Para i) usamos el teorema de Gauss: Si $x \geq 0$, entonces $4x+1 = 4^0u$ y es fácil ver que $u = 4x + 1 \not\equiv 7 \bmod(8)(4x + 1 \equiv 1, 5 \bmod(8))$. Por Gauss $4x + 1$ es la suma de tres cuadrados. En la otra dirección $4x + 1 \geq 0$ luego $x \geq 0$. R. Robinson también probó que es imposible definir $\{x \geq 0\}$ en $\mathbb{Z}$ con un sólo cuantificador.

(11) (J. ROBINSON). Dados $r_i \in \mathbb{Q}$ distintos $1 \leq i \leq n$, existe $f(t) \in \mathbb{Q}(t)$ tal que:
(i) $f(t) = 0 \Leftrightarrow t = r_i \quad i = 1, \ldots, n.$
(ii) $f^2(t) \leq (t - r_i)^2 \quad \forall t \quad$ y cada $\quad i.$
Solución: Tome

$$f(t) = c\left(\frac{(t-r_1)(t-r_2)\cdots(t-r_n)}{1+(t-r_1)^2\cdots(t-r_n)^2}\right)$$

con $c \in \mathbb{Q}$, $c > 0$ suficientemente pequeño.

(12) Sea K un campo de característica cero y $\alpha \neq 0$ en K.
a) Verifique que si a, b satisfacen la ecuación $a^3 + b^3 = \alpha$ entonces

$$x = \frac{12\alpha}{a+b}, \qquad y = 36\alpha\left(\frac{a-b}{a+b}\right) \quad \text{satisfacen la ecuación} \quad y^2 = x^3 - 2^4 3^3 \alpha^2$$

b) Verifique que si x, y están en K y satisfacen la ecuación $y^2 = x^3 - 2^4 3^3 \alpha^2$ entonces $a = \dfrac{36\alpha + y}{6x}, \quad b = \dfrac{36\alpha - y}{6x}$ satisfacen la ecuación $a^3 + b^3 = \alpha$.
En el lenguaje de curvas, las curvas son biracionalmente equivalentes.

(13) Sea K un campo de característica cero y $\alpha \neq 0$ en K.
a) Demuestre que si $f, g \in K(t)$ y satisfacen $f^3 + g^3 = \alpha$ entonces $f, g \in K$.
Solución: Si f, g satisfacen la ecuación, tenemos entonces polinomios primos entre si $p, q, r \in K[t]$ tales que $p^3 + q^3 + r^3\alpha^3 = 0$. Derivando esta ecuación, obtenemos $p'p^2 + q'q^2 - \alpha r'r^2 = 0$. Considerando estas dos ecuaciones como un sistema lineal homogéneo con matriz de coeficientes

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

Obtenemos: p^2 divide a $qr' - rq'$, q^2 divide a $rp' - pr'$ y r^2 divide a $pq' - qp'$.
Estas divisiones ocurren en el anillo de polinomios. Considere ahora una comparación de grados y obtenga el resultado.
b) Demuestre que si $f, g \in K(t)$ y $f^2 = g^3 - 4$, entonces f y g son constantes.

Sería interesante obtener este resultado sin usar el ejercicio 12 y la parte a). Eso es lo que intente orginalmente en el cursillo.

Bibliografía

[1] J. AX, *Solving diophantine equations modulo every prime*, Annals of Math. **85** (1967).
[2] J. DENEF, *The diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978).

[3] B. Mazur, *The topology of rational points*, Jour. of Experimental Mathematics, **1** (1992).
[4] A. Nerode, *A decision method for p–adic integral zeros of diophantine equations*, Bulletin of the Amer. Math. Soc. **69** (1963).
[5] T. Pheidas, *An effort to prove that the existential theory of $\mathbb{Q}$ is undecidable*, en Contemporary Mathematics AMS **270** (2000).
[6] T. Pheidas, *Endomorphisms of elliptic curves and undecidability in function fields of positve characteristic*, Journal of Algebra **273** (2004).
[7] B. Poonen, *Hilbert's Tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$*, J. Amer. Math. Soc. **16** (4) (2003).
[8] J. Robinson, *Definability and decision problems in arithmetic*, Jour. Symbolic Logic **14** (1949).
[9] R. Robinson, *The undecidability of pure transcendental extensions of real fields*, Zeit. Math. Logik und Grund. der Math. **10** (1964).
[10] J. Silverman. *The arithmetic of elliptic curves*. Springer–Verlag, NY, 1986.
[11] C. Videla, *The undecidability of cyclotomic towers*, Proc. Amer. Math. Soc. **128** (12) (2000).
[12] K. Zahidi, G. Corneliesen, *Complexity of undecidable formulae in the rationals and inertial Zsigmondy theorems for elliptic curves*, se encuentra en la red: ArXiv.math.NT/0412473.

(Recibido en abril de 2006. Aceptado para publicación en diciembre de 2006)

CINVESTAV–IPN
México D.F., México
e-mail: cvidela@math.cinvestav.mx