15 Ecuaciones diofánticas.

Pablo Pasarín López

"Es imposible encontrar la forma de convertir un cubo en la suma de dos cubos, una potencia cuarta en la suma de dos potencias cuartas, o en general cualquier potencia mayor que el cuadrado en la suma de dos potencias de la misma clase. Descubrí para este hecho una demostración excelente, pero este margen es demasiado pequeño para contenerla."

- Pierre Fermat.

1. Introducción

Recibe el nombre de ecuación diofántica cualquier ecuación algebraica $f(x_1, x_2, \ldots, x_n) = 0$, donde f es un polinomio de n variables con coeficientes enteros. Una solución es una n-upla de números enteros $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ que verifica la ecuación anterior.

Resolver una ecuación diofántica consiste en resolver tres problemas: decidir si el conjunto de soluciones es vacío o no; si no es vacío, determinar si es finito o infinito; si es finito, se trata de escribir una lista de sus elementos, y si es infinito, parametrizarlo. Incluso empleando las técnicas más sofisticadas de la geometría algebraica aritmética, apenas se conoce alguna solución parcial del problema planteado de esta manera.

Este tipo de ecuaciones deben su nombre al matemático griego del siglo III Diofanto de Alejandría. Uno de los problemas que Diofanto introdujo fue la ecuación diofántica $x^2 = 1 + dy^2$ con d entero (llamada ecuación de Pell).

El matemático hindú Brahmagupta fue el primero en dar una solución general a la ecuación diofántica lineal, $ax + by = c$ con a y b primos entre sí. Por otro lado, Bhaskara resolvió la ecuación de Pell para algunos casos particulares, y Lagrange en el siglo XVIII dio una solución completa para todos los casos.

En los estudios de las ecuaciones diofánticas de grado superior a dos con dos incógnitas, A. Thue demostró en el siglo XIX que si $n \geq 3$ y $a_0, a_1, \ldots, a_n, c \in \mathbb{Z}$, la ecuación

$$a_0 x^n + a_1 x^{n-1} y + a_2 x^{n-2} y^2 + \ldots + a_n y_n = c$$

no tiene solución siempre que el polinomio $p(t) = a_0 t^n + a_1 t^{n-1} + \ldots + a_{n-1} t + a_n$ sea irreducible en $\mathbb{Q}$.

Cuando aumentamos el número de incógnitas nos encontramos con uno de los problemas más famosos de la historia de las matemáticas: la Conjetura de Fermat, que data del siglo XVII. Fermat dejó una nota al margen de uno de los libros de la *Arithmetica* de Diofanto anunciando que la ecuación $x^n + y^n = z^n$ no tenía solución entera para $n > 2$. Pasaron tres siglos hasta que en 1995 Wiles demostró la tesis de Fermat.

En 1902 Hilbert publicó una colección de problemas que marcaría el rumbo de gran parte de la investigación matemática del siglo XX. El décimo problema consistía en estudiar si existe un algoritmo que permita decidir si una ecuación diofántica tiene solución en $\mathbb{Z}^n$. Matijasevich demostró 70 años después que tal algoritmo no existe.

Antes de comenzar el estudio de los tipos de ecuaciones diofánticas, el lector podrá comprobar que todos los métodos conocidos para determinar la existencia de solución solo se pueden aplicar a un tipo concreto de ecuación, no existe generalización.

2. Ecuaciones diofánticas lineales

2.1 La ecuación $ax + by = c$.

2.1.1 Teorema. La condición necesaria y suficiente para que la ecuación $ax + by = c$, con $a, b, c \in \mathbb{Z}$ tenga solución en $\mathbb{Z}$ es que $\text{mcd}(a, b)|c$ (el máximo común divisor de a y b divida a c). Si (x_0, y_0) es una solución particular de esta ecuación, cualquier otra solución viene dada por:

$$\begin{cases} x &= x_0 + \left(\frac{b}{d}\right)\lambda \\ y &= y_0 - \left(\frac{a}{d}\right)\lambda \end{cases} \qquad \text{con } \lambda \in \mathbb{Z}$$

Demostración.

1. Supongamos que (x_0, y_0) es una solución entera, es decir, $ax_0 + by_0 = c$. Sea $d = \text{mcd}(a, b)$, entonces existen a' y b' con $\text{mcd}(a', b') = 1$ tales que $da' = a$ y $db' = b$. Sustituyendo, $da'x_0 + db'y_0 = d(a'x_0 + b'y_0) = c$, lo que implica que $d|c$.
   Para la condición suficiente, supongamos que $d = \text{mcd}(a, b)$ divide a c. Entonces existe c' tal que $dc' = c$. Por la identidad de Bezout existen $r, s \in \mathbb{Z}$ tales que $ar + bs = d$. Ahora, multiplicando por c', se obtiene $c'ar + c'bs = c'd = c$. Tomando $x_0 = c'r$ e $y_0 = c's$ obtenemos una solución entera de la ecuación.
2. Para la segunda parte, por ser (x_0, y_0) una solución particular, $ax_0 + by_0 = c$. Si (x_1, y_1) es cualquier otra solución, $ax_1 + by_1 = c$, y al restar ambas ecuaciones
$$a(x_1 - x_0) = b(y_0 - y_1)$$
$$da'(x_1 - x_0) = db'(y_0 - y_1)$$
$$a'(x_1 - x_0) = b'(y_0 - y_1)$$
   Como $a'|b'(y_0 - y_1)$ y $\text{mcd}(a', b') = 1$, entonces $a'|y_0 - y_1$ y existe λ tal que $y_0 - y_1 = a'\lambda$. De este modo, $y_1 = y_0 - a'\lambda$ y sustituyendo, $a'(x_1 - x_0) = a'b'\lambda$, es decir, $x_1 = x_0 + b'\lambda$.
   Recíprocamente, si (x_0, y_0) es una solución particular, entonces $(x, y) = (x_0 + b'\lambda, y_0 - a'\lambda)$ para cada $\lambda \in \mathbb{Z}$ es solución de la ecuación ya que $ax + by = a(x_0 + \frac{b}{d}\lambda) + b(x_0 - \frac{a}{d}\lambda) = ax_0 + by_0 = c$.

■

2.2 La ecuación lineal con n incógnitas.

2.2.1 Teorema. La condición necesaria y suficiente para que la ecuación

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c \tag{15.1}$$

con $a_1, \ldots, a_n, c \in \mathbb{Z}$ tenga solución en $\mathbb{Z}$ es que $\text{mcd}(a_1, \ldots, a_n)|c$.

Demostración.

Por inducción sobre n. El caso $n = 1$ es trivial, y de hecho para $n = 2$ ya está probado. Supongamos que se cumple la proposición para $n - 1$. Sea $d = \text{mcd}(a_1, \ldots, a_{n-1})$, aplicando la hipótesis de inducción, $a_1x_1 + \ldots + a_{n-1}x_{n-1} = c - a_nx_n$ tiene solución si y solo si $d|c - a_nx_n$. Por lo tanto, existe $\alpha \in \mathbb{Z}$ tal que $d\alpha = c - a_nx_n$, que tendrá solución si y solo si $\text{mcd}(d, a_n)|c$. Como $\text{mcd}(d, a_n) = \text{mcd}(a_1, \ldots, a_n)$, entonces la ecuación (15.1) tiene solución si y solo si $\text{mcd}(a_1, \ldots, a_n)|c$. ■

2.2.2 Corolario. Si la ecuación $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$, con $a_1, a_2, \ldots, a_n, c \in \mathbb{Z}$ tiene una solución entonces tiene infinitas.

Demostración.

Basta considerar una solución y poner la ecuación en función, por ejemplo, de las dos primeras incógnitas, x_1 y x_2, y aplicando el teorema 2.1.1, el resultado es inmediato. ■

3. Sistemas de ecuaciones diofánticas lineales

3.1 Teorema chino del resto. Sean $n_1, n_2, \ldots, n_k \in \mathbb{N}$ tales que $\text{mcd}(n_i, n_j) = 1$ para todo $i \neq j$, es decir, primos entre sí. Sean $a_1, a_2, \ldots, a_k \in \mathbb{Z}$, entonces el sistema

$$\begin{cases} x & \equiv & a_1 \ (\text{mód } n_1) \\ x & \equiv & a_2 \ (\text{mód } n_2) \\ \vdots & & \\ x & \equiv & a_k \ (\text{mód } n_k) \end{cases}$$

tiene solución para $x \in \mathbb{Z}$. Además, si $n = n_1 \cdot n_2 \cdots n_k$, entonces todas las soluciones son congruentes módulo n.

Demostración.

Sea $n_1 \cdot n_2 \cdots n_k$ el producto de los k números primos entre sí. Sea $q_i = \frac{n}{n_i}$ para $i = 1, 2, \ldots, k$. Como $\text{mcd}(q_i, n_i) = 1$, existe r_i inverso de q_i en $\mathbb{Z}_{n_i}$, es decir, $q_i r_i \equiv 1 \ (\text{mód } n_i)$ para $i = 1, 2, \ldots, k$. Ahora definimos el número entero x por

$$x = \sum_{i=1}^{k} a_i q_i r_i = a_1 q_1 r_1 + a_2 q_2 r_2 + \ldots + a_k q_k r_k$$

De este modo, como $n_i | q_j$ para $i \neq j$, entonces $x \equiv a_i q_i r_i \ (\text{mód } n_i)$. Además, $q_i r_i \equiv 1 \ (\text{mód } n_i)$, entonces $x \equiv a_i \ (\text{mód } n_i)$ para todo $i = 1, 2, \ldots, k$.

Sea y otra solución, $y \equiv a_i \ (\text{mód } n_i)$ para todo $i = 1, 2, \ldots, k$, entonces $n_i | x - y$ para todo $i = 1, 2, \ldots, k$, lo cual implica que $\text{mcm}(n_1, n_2, \ldots, n_k) | x - y$, es decir $x \equiv y \ (\text{mód } n)$. ■

3.1.1 Observación. La demostración anterior nos proporciona un método para resolver las ecuaciones en congruencias. Es una demostración constructiva.

3.2 Sistemas de ecuaciones lineales $AX = C$. Consideremos el sistema de ecuaciones lineales diofánticas $\sum_{j=1}^{n} a_{ij} x_j = c_i$ para $i = 1, \ldots, m$. Sean $A = (a_{ij}) \in \mathcal{M}_{m \times n}(\mathbb{Z})$ y $C = (c_i) \in \mathcal{M}_{n \times 1}(\mathbb{Z})$ tal que el sistema se escribe matricialmente como $AX = C$.

3.2.1 Teorema. Las condiciones necesarias para que el sistema $AX = C$ tenga solución entera son:

1. $\text{rang}(A) = \text{rang}(A|C)$, donde $(A|C)$ es la matriz ampliada del sistema.
2. c_i es **múltiplo** de $\text{mcd}(a_{i1}, \ldots, a_{in})$ para cada $i = 1, \ldots, m$.

Demostración.

La primera se deduce del teorema de Rouche y la segunda de 2.2.1. ■

3.2.2 Teorema de Steinitz. La condición necesaria y suficiente para que el sistema diofántico lineal $AX = C$ tenga solución entera es que $\text{rang}(A) = \text{rang}(A|C) = r$ y el máximo común divisor de todos los menores de orden r de la matriz A divida a todos los menores de orden r de la matriz $(A|C)$.

4. Ecuaciones diofánticas de segundo grado

4.1 La ecuación de Pell: $x^2 - dy^2 = 1$. Si d es negativo pero distinto de -1 o es positivo pero cuadrado perfecto, entonces es inmediato que las únicas soluciones son $x = \pm 1$ y $y = 0$. El caso $d = -1$ también es evidente: ya sea $x = \pm 1$ y $y = 0$ o bien $x = 0$ y $y = \pm 1$. El caso general, en el que d es positivo sin ser un cuadrado perfecto, fue resuelto por Lagrange. El método consiste en expresar $\sqrt{d}$ en forma de fracción continua para calcular la solución natural más pequeña (x_0, y_0). A partir de ahí se demuestra que el número de soluciones es

infinito y que estas se pueden obtener a partir de $x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^n$ para cada $n \in \mathbb{N}$.

4.2 La ecuación $x^2 - y^2 = n$.

4.2.1 Teorema. La condición necesaria y suficiente para que la ecuación $x^2 - y^2 = n$ con $n \in \mathbb{N}$ tenga solución en los números enteros es que n se pueda factorizar como producto de dos números a y b de la misma paridad, es decir, ambos pares o ambos impares. En ese caso, las soluciones son:

$$x = \frac{a+b}{2}, \quad y = \frac{a-b}{2}$$

donde a y b recorren todos los pares de enteros de igual paridad.

Demostración.

Comencemos con la condición necesaria. Podemos escribir:

$$x^2 - y^2 = (x-y)(x+y) = n$$

Si x e y tienen la misma paridad, entonces $x+y$ y $x-y$ son pares. Si x e y tienen distinta paridad, entonces $x+y$ y $x-y$ son impares. En ambos casos la suma y la diferencia tienen la misma paridad.

Por otro lado, supongamos que n se puede descomponer en $n = ab$ con $a, b \in \mathbb{Z}$ de la misma paridad. Entonces

$$\begin{cases} x+y &= a \\ x-y &= b \end{cases}$$

y dado que $a+b$ y $a-b$ son pares, existen los enteros $x = \frac{a+b}{2}$ e $y = \frac{a-b}{2}$. ■

4.2.2 Observaciones.

1. Esta caracterización también puede enunciarse con la condición de que n sea impar o múltiplo de 4. Si n es impar, entonces a y b son impares. Por otro lado, si n es par resulta que:
   a) Si n no es múltiplo de 4, la ecuación no tiene solución ya que a y b no tienen la misma paridad.
   b) Si n es múltiplo de 4, entonces $n = 4n'$, $a = 2a'$ y $b = 2b'$. De este modo, $n' = a'b'$, y las soluciones son $x = a' + b'$ e $y = a' - b'$.

   En particular, si n es un cuadrado perfecto entonces o bien es impar, ya que al elevar al cuadrado se conserva la paridad, o bien es múltiplo de 4 ya que los cuadrados de los pares son múltiplos de 4. En este caso estamos diciendo que la ecuación del tipo $x^2 = z^2 + y^2$, que como veremos más adelante se llama ecuación pitagórica, tiene solución en los enteros.
2. Factorizar un entero impar n equivale a resolver la ecuación. Basándose en esto, Fermat ideó un algoritmo para factorizar un número natural $n \geq 3$ impar como producto de primos.

4.3 La ecuación $x^2 + y^2 = n$.

Terminamos esta sección con un importante resultado demostrado por Fermat.

4.3.1 Teorema. La condición necesaria y suficiente para que un número n pueda descomponerse como suma de dos cuadrados es que todo divisor primo de n, congruente con 3 módulo 4, debe aparecer elevado a una potencia par en la descomposición factorial de n.

4.3.2 Observación. Un número n es suma de dos cuadrados si y sólo si cada divisor primo de su descomposición factorial elevado a una potencia impar, es o bien congruente con 1 módulo 4 o bien igual a 2.

4.3.3 Ejemplo. 16200 se factoriza como $2^3 \cdot 3^4 \cdot 5^2$. Se cumple que el único divisor primo congruente con 3 (mód 4) es 3 y su exponente es par, entonces 16200 se puede descomponer en suma de dos cuadrados, $x^2 + y^2 = 16200$. Pasando las potencias pares al primer miembro y operando, $\left(\frac{x}{2\cdot 3^2\cdot 5}\right) + \left(\frac{y}{2\cdot 3^2\cdot 5}\right) = 2$. Es inmediato que para $n = 2$, la descomposición es $1^2 + 1^2$. Por lo tanto, $x = 2 \cdot 3^2 \cdot 5 = 90 = y$.

4.4 La ecuación pitagórica $x^2 + y^2 = z^2$.

Se trata de encontrar todos los triángulos rectángulos cuyos lados tengan dimensiones enteras. La solución completa del problema aparece por primera vez en la obra de

Elementos de Euclides.

4.4.1 Proposición. Si (x_0, y_0, z_0) es una solución de $x^2 + y^2 = z^2$, entonces también lo es $(\lambda x_0, \lambda y_0, \lambda z_0)$ para cada $\lambda \in \mathbb{Z}$.

4.4.2 Observación. Si $d = \text{mcd}(x_0, y_0, z_0)$, entonces $(\frac{x_0}{d}, \frac{y_0}{d}, \frac{z_0}{d})$ también es solución y además $\text{mcd}(\frac{x_0}{d}, \frac{y_0}{d}, \frac{z_0}{d}) = 1$. Este resultado, junto con el hecho de que las incógnitas estén elevadas al cuadrado, nos permite escoger entre todas las soluciones, aquellas en las que (x_0, y_0, z_0) son naturales, y además $\text{mcd}(x_0, y_0, z_0) = 1$. Llamadas **ternas pitagóricas**, ya que las demás soluciones se forman a partir de estas multiplicándolas por un número entero.

4.4.3 Teorema. Las soluciones naturales (x_0, y_0, z_0) de la ecuación pitagórica $x^2+y^2 = z^2$ tales que $\text{mcd}(x_0, y_0, z_0) = 1$ son:

$$\begin{cases} x &= 2mn \\ y &= m^2 - n^2 \\ z &= m^2 + n^2 \end{cases}$$

donde m y n son dos números naturales de distinta paridad tales que $m > n$ y $\text{mcd}(m, n) = 1$.

Demostración.

Sea $(x_0, y_0, z_0) \in \mathbb{N}^3$ una solución de la ecuación $x^2 + y^2 = z^2$ tal que $\text{mcd}(x_0, y_0, z_0) = 1$. Si x_0 y y_0 son pares, existen $p, q \in \mathbb{N}$ tales que $x_0 = 2p$ y $y_0 = 2q$.

$$z_0^2 = x_0^2 + y_0^2 = (2p)^2 + (2q)^2 = 4(p^2 + q^2)$$

Lo que implica que $4|z_0^2$, entonces $2|z_0$ y z_0 es par. Llegamos a una contradicción ya que en ese caso $\text{mcd}(x_0, y_0, z_0) \neq 1$. Por otro lado, si x_0 y y_0 son impares, existen $p, q \in \mathbb{N}$ tales que $x_0 = 2p + 1$ y $y_0 = 2q + 1$.

$$z_0^2 = (2p + 1)^2 + (2q + 1)^2 = 2[2(p^2 + p + q^2 + q) + 1]$$

Llegando a que $z_0^2/2$ es impar. Ahora, si z_0 es par, existe $t \in \mathbb{N}$ tal que $z_0 = 2t$, entonces $z_0^2/2 = 2t^2$ es par, llegando a una contradicción. Por otro lado, si z_0 es impar, existe $t \in \mathbb{N}$ tal que $z_0 = 2t + 1$, entonces $z_0^2 = (2t + 1)^2 = 4t^2 + 4t + 1$ es impar, llegando a una contradicción. En definitiva, no es posible que x_0 y y_0 tengan la misma paridad.

Partimos entonces de que x_0 es par y y_0 es impar. La otra posibilidad es simétrica. En ese caso, z_0 es impar, por lo que $z_0 + y_0$ y $z_0 - y_0$ son pares, entonces existen p, q tales que $z_0 + y_0 = 2p$ y $z_0 - y_0 = 2q$.

$$x_0^2 = z_0^2 - y_0^2 = (z_0 + y_0)(z_0 - y_0) = 4pq$$

Supongamos que p y q no son primos entre sí, es decir, que existe $d \in \mathbb{N}$ con $d|p$ y $d|q$. Entonces $d|p + q$ y $d|p - q$. Ahora

$$\begin{cases} 2p + 2q &= (z_0 + y_0) + (z_0 - y_0) = 2z_0 \\ 2p - 2q &= (z_0 + y_0) - (z_0 - y_0) = 2y_0 \end{cases} \implies \begin{cases} p + q &= z_0 \\ p - q &= y_0 \end{cases}$$

Por lo que $d|z_0$ y $d|y_0$, llegando a una contradicción ya que x_0, y_0 y z_0 eran primos entre sí. Conclusión, $\text{mcd}(p, q) = 1$.

Por otro lado, como $x_0^2 = 4pq$, entonces $(x_0/2)^2 = pq$, es decir, pq es un cuadrado perfecto. Si k es un factor primo de p entonces k^2 tiene que ser factor de p ya que k no puede dividir a q. Por lo tanto, p es necesariamente un cuadrado perfecto: $p = m^2$, para cierto $m \in \mathbb{N}$. Razonando análogamente con q, se obtiene $q = n^2$ para cierto $n \in \mathbb{N}$. De este modo, $(x_0/2)^2 = pq = m^2n^2$, y de aquí $x_0 = 2mn$.

$$\begin{cases} z_0 + y_0 &= 2m^2 \\ z_0 - y_0 &= 2n^2 \\ x_0 &= 2mn \end{cases} \implies \begin{cases} x_0 &= 2mn \\ y_0 &= m^2 - n^2 \\ z_0 &= m^2 + n^2 \end{cases}$$

Si $d \in \mathbb{N}$ con $d|m$ y $d|n$, entonces $d^2|m^2$, $d^2|n^2$, pero esto no es posible ya que si no $d^2|p$ y $d^2|q$. Por lo tanto, $\text{mcd}(m, n) = 1$.

Además, si m y n tuvieran la misma paridad, y_0 no podría ser impar. Para finalizar, como $2p > 2q$, entonces $m > n$.

Para la condición suficiente, supongamos que

$$\begin{cases} x &= 2mn \\ y &= m^2 - n^2 \\ z &= m^2 + n^2 \end{cases}$$

con $m > n > 0$, $\text{mcd}(m,n) = 1$ y m y n de distinta paridad. Entonces

$$x^2 + y^2 = (2mn)^2 + (m^2 - n^2)^2 = 4m^2n^2 + m^4 + n^4 - 2m^2n^2 = m^4 + n^4 + 2m^2n^2 = (m^2 + n^2)^2$$

es solución. Además, la terna $(2mn, m^2 - n^2, m^2 + n^2)$ es **pitagórica**, es decir, son primos entre sí. En efecto, supongamos que d es divisor primo de x, y y z, entonces, por ser z impar, $d \neq 2$. Como $d|y$, entonces $d|z + y$ y también $d|z - y$. Pero $z + y = 2m^2$ y $z - y = 2n^2$, entonces $d|2m^2$ y $d|2n^2$. Ya sabemos que d no es 2, por lo que $d|m^2$ y $d|n^2$. Como además es primo, $d|m$ y $d|n$, lo cual no es posible ya que $\text{mcd}(m,n) = 1$.

En definitiva, la terna anterior es pitagórica y todas las soluciones enteras de $x^2 + y^2 = z^2$ son de la forma:

$$\begin{cases} x &= 2\lambda mn \\ y &= \lambda(m^2 - n^2) \qquad \text{con } \lambda \in \mathbb{Z} \\ z &= \lambda(m^2 + n^2) \end{cases}$$

■

5. Ecuaciones diofánticas de grado mayor que dos

5.1 Ecuaciones con una incógnita. El objetivo es determinar las raíces enteras de un polinomio

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$$

5.1.1 Lema de Gauss. Se llama **contenido** del polinomio $f \in \mathbb{Z}[x]$, y se denota por $c(f)$, al máximo común divisor de los coeficientes de f. Si $f, g, h \in \mathbb{Z}[x]$ y $f = gh$, se cumple que $c(f) = c(g)c(h)$.

5.1.2 Proposición. Sean $u, v \in \mathbb{Z}$ tales que $\text{mcd}(u,v) = 1$, y $\frac{u}{v} \in \mathbb{Q}$ una raíz del polinomio anterior, entonces

1. u divide a a_0 y v divide a a_n.
2. $v - u$ divide a $s(f) = a_0 + a_1 + \ldots + a_n$ y $u + v$ divide a $t(f) = a_0 - a_1 + \ldots + (-1)^n a_n$.

Demostración.

1. Eliminando los denominadores en la igualdad $p(\frac{u}{v}) = 0$,
$$(a_1 v^{n-1} + \ldots + a_{n-1} v u^{n-2} + a_n u^{n-1})u = -a_0 v^n$$
De aquí se deduce que u divide a $a_0 v^n$, y como u es primo con v, entonces u divide a a_0. Además, v divide la suma $a_1 v^{n-1} + \ldots + a_{n-1} u^{n-2} v + a_n u^{n-1}$, y como divide a los $n-1$ primeros sumandos, también divide a $a_n u^{n-1}$, por lo que divide a a_n.
2. Aplicando la regla de Ruffini en $\mathbb{Q}[x]$, existe un polinomio con coeficientes racionales $h \in \mathbb{Q}[x]$ tal que $f = (x - \frac{u}{v})h$. Si d es el mínimo común múltiplo de los denominadores de los coeficientes de h, entonces $dh = g \in \mathbb{Z}[x]$, y
$$vdf = vd\Big(x - \frac{u}{v}\Big)h = (vx - u)g$$
Como u y v son primos entre sí, el contenido del polinomio $vx - u$ es 1, entonces, por el Lema de Gauss,
$$vdc(f) = c(vdf) = c(vx - u)c(g) = c(g)$$
Sacando el factor común $c(g)$ en g, $g = c(g)g_1$ para cierto $g_1 \in \mathbb{Z}[x]$, entonces sustituyendo
$$vdf = (vx - u)c(g)g_1 = (vx - u)vdc(f)g_1$$
Simplificando, $f = (vx - u)c(f)g_1$. De este modo, resulta que $f(1) = s(f)$ es múltiplo de $v - u$ y que

$f(-1) = t(f)$ es múltiplo de $u + v$.

■

Empleando la primera parte de la proposición en el caso $a_n = 1$, y la segunda en el caso $v = 1$, obtenemos el siguiente resultado.

5.1.3 Corolario: Raíces enteras de polinomios con coeficientes enteros.

1. Las raíces racionales de un polinomio mónico con coeficientes en $\mathbb{Z}$ son números enteros.
2. El conjunto de raíces enteras de f es un subconjunto del conjunto finito

$$F = \{u \in \mathbb{Z} : u \text{ divide a } a_0, u-1 \text{ divide a } s(f) \text{ y } u+1 \text{ divide a } t(f)\}$$

5.2 Ecuaciones con tres o más incógnitas.

La pregunta sobre la existencia de una cantidad finita o infinita de soluciones en $\mathbb{Z}$, o sobre su cálculo explícito, para ecuaciones de grado mayor que dos y más de dos incógnitas tiene respuesta solo para clases particulares de ecuaciones. Entre ellas, la famosa:

$$x^n + y^n = z^n$$

5.2.1 Último Teorema de Fermat. Fermat utilizando el método de **descenso infinito** demostró que para $n = 4$ la ecuación no tiene solución en los enteros y conjeturó que no existe ninguna para $n > 2$:

"Es imposible encontrar la forma de convertir un cubo en la suma de dos cubos, una potencia cuarta en la suma de dos potencias cuartas, o en general cualquier potencia mayor que el cuadrado en la suma de dos potencias de la misma clase. Descubrí para este hecho una demostración excelente, pero este margen es demasiado pequeño para que quepa en él."

En los años 80 Faltings demostró que si $n > 2$ el conjunto de soluciones es finito, y en los años 90 Andrew Wiles demostró apoyándose en la teoría de curvas elípticas y formas modulares que de hecho es vacío.

5.3 La ecuación $x^4 + y^4 = z^4$.

5.3.1 Teorema. La ecuación $x^4 + y^4 = z^2$ no tiene solución dentro del conjunto de los enteros.

Demostración.

Supongamos, por reducción al absurdo, que (x_0, y_0, z_0) es una solución. Sea $d = \text{mcd}(x_0, y_0)$, entonces existen x_d y y_d tales que $\text{mcd}(x_d, y_d) = 1$ con $dx_d = x_0$ y $dy_d = y_0$. Sustituyendo, se obtiene $z_0^2 = d^4(x_d^4 + y_d^4)$, lo cual implica que $d^4 | z_0^2$. Ahora, existe z_0^* tal que $d^4 z_0^* = z_0^2$, por lo que $z_0^* = \left(\frac{z_0}{d^2}\right)^2$. Por lo tanto, z_0^* es un cuadrado perfecto, $z_0^* = z_d^2$.

$$\begin{aligned} d^4 z_d^2 &= d^4(x_d^4 + y_d^4) \\ z_d^2 &= (x_d^2)^2 + (y_d^2)^2 \end{aligned}$$

Como x_d y y_d son primos entre sí, también lo son x_d^2 y y_d^2. Por el teorema 4.4.3 existen m, n de distinta paridad y $\text{mcd}(m, n) = 1$, tales que:

$$\begin{cases} x_d &= 2mn \\ y_d &= m^2 - n^2 \\ z_d &= m^2 + n^2 \end{cases}$$

Si m es par y n impar, $m = 2m_d$ y $n = 2n_d$. De este modo, empleando la teoría de congruencias y considerando las clases módulo 4:

$$\begin{aligned} y_d^2 &= 4m_d^2 - 4n_d^2 - 4n_d - 1 \\ [y_d^2]_4 &= [-1]_4 = [3]_4 \end{aligned}$$

Análogamente,

$$\begin{aligned} z_d^2 &= 4m_d^2 + 4n_d^2 + 4n_d + 1 \\ [z_d^2]_4 &= [1]_4 \\ x_d^2 &= 8m_d n_d + 4m_d \\ [x_d^2]_4 &= [0]_4 \end{aligned}$$

Llegamos a una contradicción, ya que $[x_d^2]_4 + [y_d^2]_4 = [0]_4 + [3]_4 \neq [1]_4 = [z_d^2]_4$. De este modo, m es impar y n par, $n = 2t$ para algún $t \in \mathbb{N}$, entonces $x_0^2 = 4mt$, lo cual implica que $mt = \left(\frac{x_0}{2}\right)^2$, y como $\text{mcd}(m,t) = 1$ ya que $\text{mcd}(m,n) = 1$, tanto m como t son cuadrados perfectos, $m = m_1^2$ y $t = t_1^2$ con $m_1, t_1 \in \mathbb{N}$.

Por otro lado, $y_0 + n^2 = m^2$ y como $\text{mcd}(y_0, m, n) = 1$, se trata de una terna pitagórica en la que n es par:

$$\begin{cases} n &= 2m'n' \\ y_0 &= m'^2 - n'^2 \\ m &= m'^2 + n'^2 \end{cases}$$

con $\text{mcd}(m', n') = 1$, $m' > n'$ y m' y n' de distinta paridad. Por lo tanto, $m'n' = \frac{n}{2} = t = t_1^2$. De este modo, m' y n' son cuadrados perfectos, $m' = x_1^2$ y $n' = y_1^2$, entonces

$$m_1^2 = m = m'^2 + n'^2 = x_1^4 + y_1^4$$

Dado que m_1 y t_1 son enteros positivos, $0 < m_1 \leq m_1^2 = m \leq m^2 < m^2 + n^2 = z_0$. De este modo, partiendo de (x_0, y_0, z_0) llegamos a (x_1, y_1, m_1) con $0 < m_1 < z_0$. Es claro que este proceso no puede continuar indefinidamente ya que no existen infinitos enteros menores que z_0 y mayores que 0, lo que implica que $x^4 + y^4 = z^2$ no tiene solución. ■

5.3.2 Corolario. La ecuación $x^4 + y^4 = z^4$ no tiene solución en $\mathbb{Z}$.

Demostración.

Si (x_0, y_0, z_0) fuera solución, entonces (x_0, y_0, z_0^2) sería solución de $x^4 + y^4 = z^2$, lo cual es imposible. ■

5.3.3 Corolario. La ecuación $x^{4n} + y^{4n} = z^{4n}$ no tiene solución en $\mathbb{Z}$ para $n \in \mathbb{N}$.

6. Conclusión

A lo largo del capítulo se tratan las ecuaciones diofánticas desde una menor a una mayor dificultad en cuanto a su resolución. Además, esta evolución es acorde con el desarrollo histórico desde la antigua Mesopotamia, pasando por la época griega de Diofanto, la época hindú de Brahmagupta y Bhaskara, hasta llegar al siglo XVI en adelante.

7. Contexto en el currículo

Aunque este tipo de ecuaciones no aparecen recogidas en el currículo de Secundaria y Bachillerato, son un recurso muy frecuente para trabajar con el alumnado de altas capacidades y para ser introducidas en concursos de lógica, en eventos de historia de las matemáticas u otros contextos matemáticos.

8. Bibliografía recomendada

An Introduction to Diophantine Equations - A Problem-Based Approach - Andreescu

Índice general