Preparación Olimpiadas Matemáticas
Ecuaciones Diofánticas

Almería, 28 de noviembre de 2015

David Crespo Casteleiro

Introducción

Se llama ecuación diofántica a cualquier ecuación algebraica con coeficientes enteros, de la que nos interesa exclusivamente las soluciones que tenga dentro del conjunto de los números enteros.
El origen del término diofántico hay que buscarlo en el matemático Diofanto de Alejandría, que vivivó en el s. III, y que se ocupó de este tipo de ecuaciones. Tanto es así que en su epitafio rezaba la siguiente leyenda:

Transeúnte, ésta es la tumba de Diofanto: es él quien con esta sorprendente distribución te dice el número de años que vivió. Su niñez ocupó la sexta parte de su vida; después, durante la doceava parte su mejilla se cubrió con el primer bozo. Pasó aún una séptima parte de su vida antes de tomar esposa y, cinco años después, tuvo un precioso niño que, una vez alcanzada la mitad de la edad de su padre, pereció de una muerte desgraciada. Su padre tuvo que sobrevivirle, llorándole, durante cuatro años. De todo esto se deduce su edad.

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 = x$$

Contenido

1. Ecuaciones con una incógnita

- La ecuación $ax = b$ tiene solución si y sólo si a|b

  Ejemplo: 3x=6 tiene por solución x=2. En cambio 3x=7 no tiene solución entera.
- Las soluciones enteras de la ecuación

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

han de encontrase entre los divisores de a_0

1. Ecuaciones con una incógnita

Ejemplo: Calcular las raíces enteras de la ecuación

$$3x^3 - x^2 - 12x + 4 = 0$$

Los candidatos a soluciones se encuentran entre

$$div(4) = \{\pm 1, \pm 2, \pm 4\}$$

$$3 \cdot 1^3 - 1^2 - 12 \cdot 1 + 4 = -6$$

$$3 \cdot (-1)^3 - (-1)^2 - 12 \cdot (-1) + 4 = 12$$

$$3 \cdot 2^3 - 2^2 - 12 \cdot 2 + 4 = 0$$

$$3 \cdot (-2)^3 - (-2)^2 - 12 \cdot (-2) + 4 = 0$$

$$3 \cdot 4^3 - 4^2 - 12 \cdot 4 + 4 = 132$$

$$3 \cdot (-4)^3 - (-4)^2 - 12 \cdot (-4) + 4 = -156$$

Soluciones x=2, -2

1. Ecuaciones con una incógnita

Teorema de la raíz racional: Las soluciones racionales de la ecuación

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

son de la forma $\frac{a}{b}$ donde $a \in div(a_0)$ y $b \in div(a_n)$

Ejemplo: Calcular las soluciones racionales de la ecuación

$$3x^3 - x^2 - 12x + 4 = 0$$

La lista de candidatos a raíces sería:

$$\pm 1, \pm \frac{1}{3}, \pm 2, \pm \frac{2}{3}, \pm 4, \pm \frac{4}{3}$$

Como puede comprobarse, las soluciones son x=2, -2 y 1/3

2. Ecuaciones con varias incógnitas

Vamos a distinguir entre el caso de que la ecuación que queremos resolver sea lineal o por el contrario no lo sea

2. 1 Ecuaciones lineales

Una ecuación lineal con dos incógnitas es una expresión de la forma $ax + by = c$ con $a, b, c \in \mathbb{Z}$.

Veamos bajo qué circunstancias tiene solución esta ecuación. Para ello, hemos de conocer un resultado conocido como **identidad de Bézout**:

Sean a, b dos números enteros y d=mcd (a, b). Entonces existen dos números enteros x e y tales que ax+by=d

2. 1 Ecuaciones lineales

El algoritmo de Euclides para el cálculo del máximo común divisor, nos sirve para encontrar los valores x e y que establece la identidad de Bézout. En efecto:

$$a = b \cdot c_1 + r_1 \qquad \text{con } r_1 < b$$
$$b = r_1 \cdot c_2 + r_2 \qquad \text{con } r_2 < r_1$$
$$r_1 = r_2 \cdot c_3 + r_3 \qquad \text{con } r_3 < r_2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-1} = r_n \cdot c_{n+1} + r_{n+1} \quad \text{con } r_{n+1} < r_n$$
$$r_n = r_{n+1} \cdot c_{n+2}$$

De estas sucesivas divisiones, se obtiene el mcd(a, b)=r_{n+1} y sustituyendo el valor de los restos, la combinación lineal

2. 1 Ecuaciones lineales

Ejemplo: Calcula mcd(18, 5) y muestra la identidad de Bézout

$$18 = 5\cdot 3 + 3 \Rightarrow 3 = 18\cdot 1 - 5\cdot 3$$
$$5 = 3\cdot 1 + 2 \Rightarrow 5 = (18\cdot 1 - 5\cdot 3) + 2 \Rightarrow 2 = 18\cdot(-1) + 5\cdot 4$$
$$3 = 2\cdot 1 + 1 \Rightarrow (18\cdot 1 - 5\cdot 3) = (18\cdot(-1) + 5\cdot 4)\cdot 1 + 1$$
$$1 = 18\cdot 2 + 5\cdot(-7) \Rightarrow x = 2, y = -7$$

Ejercicios: Calcular el mcd de cada pareja de números y expresarlo como combinación lineal de estos

- 17 y 14 (sol: mcd(17, 14)=1 y 17·5+14·(-6)=1)
- 1769 y 551 (sol: mcd(1769, 551)=29 y
- 1769·5+551·(-16)=29)

2. 1 Ecuaciones lineales

Teorema: La ecuación diofántica lineal $ax+by=c$ tiene solución si y sólo si $d=\text{mcd}(a, b)\mid c$

2. 1 Ecuaciones lineales

Demostración:

=>) Supongamos que la ecuación $ax+by=c$ tiene solución. Como $d=mcd(a, b)$, existen a', b' números enteros tales que $a=a'd$, $b=b'd$. Sustituyendo en la ecuación: $a'dx+b'dy=c$ => $d(a'x+b'y)=c$ y por tanto $d|c$

<=) Supongamos $d|c$. Entonces existe un entero c' talque $c=c'd$. Pero la identidad de Bézout garantiza la existencia de dos enteros x_0 e y_0 tales que $ax_0+by_0=d$. Multiplicando esta ecuación por c', se tiene $c'ax_0+c'by_0=c'd=c$. Por lo que $x= c'x_0$, $y=c'y_0$ es una solución

2. 1 Ecuaciones lineales

La demostración del teorema anterior, nos da la clave para buscar una solución particular de una ecuación diofántica o por el contrario nos dirá si no tiene solución.

Ejemplo: La ecuación $5x+3y=16$ tiene solución ya que $mcd(5, 3)=1|16$. Además como por el algoritmo de Euclides $5\cdot(-1)+3\cdot 2=1$, multiplicando la ecuación por 16 tenemos: $5\cdot(-16)+3\cdot(32)=16$, luego una solución de la misma es $x_0=-16$, $y_0=32$.

Ejemplo: La ecuación $2x+10y=1$ no tiene solución porque $mcd(2, 10)=2$ y no divide a 1.

2. 1 Ecuaciones lineales

Teorema: Si d=mcd(a, b), d|c y x_0 e y_0 son una solución de la ecuación diofántica lineal ax+by=c , entonces las soluciones vienen dadas por:

$$\left.\begin{aligned} x &= x_0 + \frac{b}{d}t \\ y &= y_0 - \frac{a}{d}t \end{aligned}\right\}$$

donde t es un número entero

2. 1 Ecuaciones lineales

Demostración:

Veamos en primer lugar que las expresiones dadas, verifican la ecuación de partida. Sustituyendo en ella:

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) =$$

$$= (ax_0 + by_0) + \left(a\frac{b}{d}t - b\frac{a}{d}t\right) = c + 0 = c$$

2. 1 Ecuaciones lineales

Para concluir con la demostración, hemos de comprobar que las soluciones son de esta forma. Supongamos que (x, y) y (x_0, y_0) son dos soluciones de la ecuación de partida. Entonces:

$$ax + by = ax_0 + by_0 \Rightarrow \quad ax - ax_0 = by_0 - by \Rightarrow$$

$$a(x - x_0) = b(y_0 - y) \Rightarrow \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$$

Pero $mcd(a, b) = d \Rightarrow mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, con lo que

$$\frac{a}{d} | (y_0 - y) \;\; y \;\; \frac{b}{d} | (x - x_0)$$

2. 1 Ecuaciones lineales

Esto equivale a decir

$$\frac{b}{d}t = (x - x_0) \Rightarrow x = x_0 + \frac{b}{d}t$$

$$\frac{a}{d}t = (y_0 - y) \Rightarrow y = y_0 - \frac{a}{d}t$$

2. 1 Ecuaciones lineales

Ejemplos:

1. Calcular todas las soluciones enteras de la ecuaciones

a) $10x+13y=2$

b) $10x-3y=15$

c) $3x-12y=4$

2. En una estafeta de correos sólo tienen sellos de 14 y 21 céntimos. ¿De qué formas puede franquear un paquete postal por importe de 7'77 euros?

2. 1 Ecuaciones lineales

3. Una bodega debe entregar un pedido de 81000 litros de vino sin embotellar. Para ello posee camiones cisterna que transportan 3500 litros cada uno y remolques cisterna que transportan 1500. Cada camión puede llevar como mucho un remolque y, lógicamente, los remolques no pueden circular solos. Además, las cisternas deben ir llenas. Si la bodega quiere minimizar el número de camiones utilizados, ¿cuántos camiones y remolques debe utilizar? ¿Y si cada camión pudiera llevar hasta dos remolques?

2. 1 Ecuaciones lineales

4. Queremos echar 21 litros de gasóleo a un depósito usando bidones de 2 y 5 litros. Responder a las siguientes cuestiones:

a) ¿Es posible? ¿Por qué?

b) En caso afirmativo, dar todas las combinaciones posibles.

5. En una bolsa hay monedas de 5, 10 y 20 céntimos. Se sabe que hay en total 24 monedas y que su valor es 2 euros. ¿Qué combinaciones de monedas son posibles?

2. 1 Ecuaciones lineales

El caso general de la ecuación diofántica de n incógnitas $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$ tiene solución entera si y sólo si $mcd(a_1, a_2, \ldots, a_n)|c$. La búsqueda de la soluciones, se resumen en encontrar las de una ecuación de dos incógnitas. Los pormenores pueden consultarse en (Sánchez-Rubio, 2000)

2. 2 Ecuaciones no lineales

Los casos que hemos anteriormente visto, ponen de manifiesto la disparidad de métodos para resolver ecuaciones diofánticas. En este sentido el matemático alemán David Hilbert, propuso en 1900 una lista de 23 problemas no resueltos hasta esa fecha. El décimo se planteaba:

"Encontrar un algoritmo que determine si una ecuación diofántica polinómica dada con coeficientes enteros tiene solución entera".

2. 2 Ecuaciones no lineales

En el año 1970, el matemático Yuri Matiyasevich demostró la imposibilidad del décimo problema: No hay ningún algoritmo capaz de determinar la resolubilidad de cualquier ecuación diofántica. Por lo tanto tampoco podremos encontrar un método general que obtenga las soluciones.

Por este motivo, trataremos casos particulares de ecuaciones que admiten un método para resolverlas. Desde luego la bibliografía aportada permite un estudio más exhaustivo.

2. 2 Ecuaciones no lineales

Vamos a distinguir dentro de las ecuaciones no lineales, el caso de que tengan dos o por el contrario más de dos incógnitas.

2.2.1 Ecuaciones con dos incógnitas

- La ecuación $x^2 - y^2 = a$

Esta ecuación puede ser escrita como $(x + y)(x - y) = a$. Llamando $x + y = m, x - y = n$ la ecuación se expresa como $m \cdot n = a$. Además m y n han de tener la misma paridad, pues la suma y la resta de dos números tienen la misma paridad. Al resolver el sistema se obtiene:

$$\left.\begin{array}{r} x + y = m \\ x - y = n \end{array}\right\} \Longrightarrow \left.\begin{array}{l} x = \dfrac{m + n}{2} \\ y = \dfrac{m - n}{2} \end{array}\right\}$$

2.2.1 Ecuaciones con dos incógnitas

Ejemplo: Resolver la ecuación $x^2 - y^2 = 8$. La ecuación $m \cdot n = 8$ arroja las siguientes posibilidades:

$$(1, 8), (8,1), (-1, -8), (-8, -1)$$
$$(2, 4), (4, 2), (-2, -4), (-4, -2)$$

Descartando las que no tienen la misma paridad, nos quedan:

$$(2, 4), (4, 2), (-2, -4), (-4, -2)$$

Deshaciendo el cambio, los valores posibles para (x,y) son:

2.2.1 Ecuaciones con dos incógnitas

m	n	$x = \frac{m+n}{2}$	$y = \frac{m-n}{2}$
2	4	3	-1
4	2	3	1
-2	-4	-3	1
-4	-2	-3	-1

Nótese que si (a, b) es una solución también lo son $(\pm a, \pm b)$

2.2.1 Ecuaciones con dos incógnitas

- La ecuación $x^2 - ay^2 = b$

Esta ecuación, donde a es un número entero que no es un cuadrado perfecto, es conocida como ecuación de Pell (aunque el nombre no es demasiado acertado ya que Pell parece ser que no fue quien la estudió) y tiene gran importancia ya que cualquier otra ecuación de segundo grado con dos incógnitas, puede ser reducida a una ecuación de Pell. Claramente tiene una solución trivial (x, y)=(1, 0). Pues bien, si encontramos cualquier otra solución distinta de esta, existe un método basado en fracciones continuas que nos proporciona el resto de soluciones y que puede seguirse en Guelfond (1979).

2.2.1 Ecuaciones con dos incógnitas

- El caso de que a sea un cuadrado perfecto es simple de resolver pues el primer miembro admite factorizarse como:

$$x^2 - ay^2 = (x - \sqrt{a}y)(x + \sqrt{a}y)$$

Y volviendo a hacer un cambio de variables

$$\left.\begin{aligned} x + \sqrt{a}y &= m \\ x - \sqrt{a}y &= n \end{aligned}\right\} \Longrightarrow \left.\begin{aligned} x &= \frac{m+n}{2} \\ y &= \frac{m-n}{2\sqrt{a}} \end{aligned}\right\}$$

La ecuación se transforma en $m \cdot n = b$

2.2.1 Ecuaciones con dos incógnitas

Para terminar este somero repaso, vamos a resolver el caso de la ecuación diofántica $P(x, y) = 0$ (1) donde P es un polinomio homogéneo de grado α, es decir:

$$P(\lambda x, \lambda y) = \lambda^{\alpha} P(x, y)$$

Este tipo de ecuación posee siempre la solución (0, 0). Descartada esta, podemos hacer un cambio de variable $\frac{y}{x} = z$ transformándose la ecuación (1) en

$$Q(z) = 0 \quad (2)$$

de la que nos interesan sus soluciones racionales. Aplicando el Teorema de la raíz racional a (2) tenemos el problema resuelto.

2.2.1 Ecuaciones con dos incógnitas

Ejemplo: Hallar las soluciones enteras de la ecuación $x^4 + y^4 = 3x^3y$.

Claramente, la ecuación tiene por solución (x, y)=(0, 0).

La ecuación dada es homogénea de grado 4. En efecto, si llamamos $P(x,y) = x^4 + y^4 - 3x^3y$ se tiene:

$$\begin{aligned} P(\lambda x, \lambda y) &= (\lambda x)^4 + (\lambda y)^4 - 3(\lambda x)^3(\lambda y) \\ &= \lambda^4 x^4 + \lambda^4 y^4 - 3\lambda^3 x^3 \lambda y = \lambda^4 P(x,y) \end{aligned}$$

2.2.1 Ecuaciones con dos incógnitas

Si suponemos $(x, y) \neq (0,0)$ y dividimos todos los términos de la ecuación por x^4 obtenemos:

$$\frac{x^4 + y^4}{x^4} = \frac{3x^3 y}{x^4} \Longrightarrow 1 + \left(\frac{y}{x}\right)^4 = 3\,\frac{y}{x}$$

Haciendo el cambio propuesto, $\frac{y}{x} = z$, la ecuación se transforma en $1 + z^4 = 3z \Longrightarrow z^4 - 3z + 1 = 0$ (1). De esta ecuación queremos conocer sus raíces racionales. El Teorema de la raíz racional afirma que los únicos candidatos a raíces son $z = \pm 1$. Pero como puede comprobarse, ninguna es solución de (1) por lo que (1) no tiene raíces racionales y por lo tanto tampoco enteras. Así la ecuación de partida no tiene más soluciones distinta de la trivial.

2.2.2 Ecuaciones con más de dos incógnitas

Terminamos este epígrafe hablando de una ecuación con tres incógnitas, conocida como ecuación de Fermat. El origen de la misma es la Conjetura de Fermat o último teorema de Fermat, cuyo enunciado es:

La ecuación $x^n + y^n = z^n$ siendo n un valor entero con $n \geq 3$ no tiene solución en números enteros positivos x, y, z (el caso xyz=0 se excluye por ser x, y, z positivos)

2.2.2 Ecuaciones con más de dos incógnitas

A pesar de que Fermat afirmó: “He encontrado una demostración maravillosa de este resultado pero este margen (de un libro) es demasiado pequeño para contenerla”, el problema estuvo abierto más de trescientos años hasta que en 1995 A. Wiles consiguió una demostración del mismo. A pesar de la no existencia de soluciones, tiene especial interés el caso n=2, por tratarse de la ecuación que aparece en el Teorema de Pitágoras.

2.2.2 Ecuaciones con más de dos incógnitas

- La ecuación Pitagórica $x^2 + y^2 = z^2$

El método para resolverla es válido para ecuaciones de segundo grado homogéneas con tres variables. Consiste en descomponer la ecuación como dos cocientes en los que el numerador y el denominador son funciones lineales. A su vez, se igualan estos al cociente entre m y n , siendo estos coprimos. Veamos cómo:

2.2.2 Ecuaciones con más de dos incógnitas

$$x^2 + y^2 = z^2 \Leftrightarrow x^2 = z^2 - y^2 \Leftrightarrow x^2 = (\mathrm{z} - \mathrm{y})(\mathrm{z} + \mathrm{y})$$

Podemos entonces escribir:

$$\frac{x}{z-y} = \frac{z+y}{x} = \frac{m}{n} \Rightarrow \begin{cases} nx = mz - my \\ mx = nz + ny \end{cases}$$

Reduciendo el sistema a una ecuación que no contenga x

$$(m^2 - n^2)z = (n^2 + m^2)y$$

Por lo tanto

$$z = n^2 + m^2, \mathrm{y} = m^2 - n^2, \mathrm{x} = 2\mathrm{mn}$$

2.2.2 Ecuaciones con más de dos incógnitas

Consideraciones

- Hay infinitas soluciones de la ecuación que dependen de m y n.
- Los valores de x e y se intercambian.
- Una vez obtenida una solución $(x, y, z) = (a, b, c)$, podemos encontrar una infinitud de otras soluciones de la forma $(x, y, z) = (\lambda a, \lambda b, \lambda c)$.
- Las soluciones de esta ecuación se llaman *ternas pitagóricas* y geométricamente son las longitudes de los lados de un triángulo rectángulo.

3. Técnicas variadas

Bajo esta definición hemos recogido algunas estrategias que pueden permitirnos obtener la solución de ecuaciones que no se adapten a los casos anteriormente descritos.

- **Método de factorización**

Consiste en factorizar uno de los miembros y a tenor de lo que ocurra en el otro, distinguir casos.

Ejemplo: Demostrar que la ecuación $2x^2 + 3xy = 7$ no tiene solución entera.

3. Técnicas variadas

$$2x^2 + 3xy = 7 \Rightarrow x(2x + 3y) = 7 \Rightarrow$$
$$x = 7, 2x + 3y = 1$$
$$x = -7, 2x + 3y = -1$$
$$x = 1, 2x + 3y = 7$$
$$x = -1, 2x + 3y = -7$$

Ninguna de estas posibilidades arroja solución

Ejercicios: Calcular las soluciones enteras

- $x + y - xy = 0$
- $2x^2 + xy - 3y^2 = 17$

3. Técnicas variadas

- **Método de la suma**

De manera similar al método de factorización, con la variante de que uno de los miembros de la ecuación es suma de potencias, considerándose los casos posibles

Ejemplo: Hallar los números cuya suma de cuadrados sea el doble de dichos números

El enunciado puede expresarse algebraicamente como

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

3. Técnicas variadas

Desarrollando y completando para obtener sendos cuadrados se tiene

$$x^2 - 2x + y^2 - 2y = 0 \Rightarrow \quad x^2 - 2x + 1 + y^2 - 2y + \\ + 1 = 2 \Rightarrow (x-1)^2 + (y-1)^2 = 2$$

Pero 2 sólo se puede expresar como suma de cuadrados en el caso $2 = (\pm 1)^2 + (\pm 1)^2$ por lo que

$$\begin{cases} x - 1 = \pm 1 \Rightarrow x = 0, 2 \\ y - 1 = \pm 1 \Rightarrow y = 0, 2 \end{cases}$$

Luego las soluciones son

$$(x, y) \in \{(0,0), (0,2), (2,0), (2,2),\}$$

Bibliografía

- Sánchez-Rubio García, C., Ripollés Amela, M. (2000) Manual de matemáticas para preparación olímpica Castelló de la Plana: Universitat Jaume I
- Guelfond, A. O., (1979) Resolución de ecuaciones en números enteros. Lecciones populares. Moscú: MIR