TEMA 15: ECUACIONES DIOFÁNTICAS

TEMA 15: ECUACIONES DIOFÁNTICAS

Como sabemos, se llama ecuación a la igualdad entre dos expresiones no equivalentes, y se llama solución a cualquier colección de valores, uno por cada incógnita, que hace que la igualdad se verifique.

Si las expresiones que constituyen una ecuación son funciones polinómicas con coeficientes enteros, y se considera encontrar únicamente las soluciones enteras, nos encontramos ante una ecuación diofántica.

Toman el nombre del matemático griego Diofanto (s. III a.C.), quien fuese uno de los primeros en introducir la notación simbólica en matemáticas. En su obra *La Arithmetica* resuelve hasta un total de 189 problemas de este tipo, cada uno de un modo distinto. A Diofanto se le ha acusado de no buscar ideas generales, sino soluciones correctas, esto es, de no profundizar suficientemente es sus métodos para generalizarlos.

El método general de resolución de ecuaciones diofánticas fue uno de los problemas que Hilbert propuso a la Comunidad Matemática en el Congreso de París en 1900. Se ha demostrado que la existencia de un algoritmo que las resuelva es indecible, es decir, no es posible encontrarlo pero tampoco se puede demostrar su no existencia.

En este estudiaré diversas ecuaciones diofánticas siguiendo el esquema expuesto anteriormente.

I. ECUACIONES DIOFÁNTICA LINEALES

I.1. ECUACIÓN LINEAL CON DOS INCÓGNITAS

Una ecuación diofántica lineal con dos incógnitas es del tipo ax+by=n donde a,b y n son números enteros. Vamos a tratar 3 problemas: existencia, forma y cálculo de las soluciones.

I.1.A. EXISTENCIA DE SOLUCIONES

Veamos una proposición que resolverá cuando una ecuación de este tipo tiene solución.

Proposición

Sean a,b, y n números enteros. La ecuación lineal ax+by=n tiene solución entera (x_0, y_0) si, y solo si, m.c.d(a,b)|n.

-Dem-

$\boxed{\Rightarrow}$ Sea d=m.c.d.(a,b). Veamos que d divide a n.

Por ser d el m.c.d.(a,b) se tiene que d|a y d|b, es decir $\exists a',b' \in Z$ tal que $\begin{cases} a=d.a' \\ b=d.b' \end{cases}$

Como (x_0,y_0) es solución de la ecuación, entonces:

$n=ax_0+by_0=d.a=x_0+db=y_0=d(a=x_0+b=y_0)$

luego d|n.

$\boxed{\Leftarrow}$ Sea el conjunto $H=\{ap+bq:\ p,q\in\mathbb{Z},\ ap+bq>0\}$ y sea d=minH>0.

Si demuestro que d=m.c.d(a,b) obtendré que:

Por hipótesis n=n=.d para cierto n= entero . Entonces como $d\in H$ existirán p_0, y q_0 enteros verificando que $n=n=(ap_0+bq_0)=a(n=p_0)+b(n=q_0)$ Luego $(n=p_0,n=q_0)$ es la solución entera buscada.

Demostremos pues que d=m.c.d(a,b).

Supongamos que d no es divisor de a, entonces como $d\neq 0$, podemos dividir a entre d. De esta forma existen $c,r\in\mathbb{Z}$ tal que a=cd+r con 0<r<d.

Por otra parte $d=ap_0+bq_0$ para determinados $p_0,q_0\in\mathbb{Z}$. Entonces:

$r=a-cd=a-c(ap_0+bq_0)=a(1-c_0)+b(-cq_0) \Rightarrow r\in H$ y r<d lo que es contradicción De esta forma obtenemos que d|a.

Análogamente, dividiendo b entre d, obtendríamos que d|b.

Veamos ahora que d es el m.c.d.(a,b):

Sea d' un divisor común de a y b

$\Rightarrow \begin{cases} a=d'p_1 \\ b=d'q_1 \end{cases} \Rightarrow$ Como $d=ap_0+bq_0=d'(p_1p_0+q_1q_0) \Rightarrow d'|d \Rightarrow mcd(a,b)=d$ ■

Obsérvese que a partir de una solución particular (p_0,q_0) de la ecuación ax+by=d donde d=m.c.d.(a,b), obtenemos una solución de la ecuación ax+by=n, $(n=p_0,n=q_0)$ donde n==n/d.

Obsérvese también que en la práctica hallar las soluciones de ax+by=n, es equivalente a hallar las soluciones de a'x+b'=n' donde a', b', y n' se han obtenido dividiendo a, b y n por d=m.c.d(a,b). Así pues no supone ninguna restricción el hecho de suponer la ecuación ax+by=n donde m.c.d (a,b)=1.

I.1.B. FORMA DE LAS SOLUCIONES

La siguiente proposición nos dirá como conseguir todas las soluciones:

Proposición

Sean a, b y n enteros no nulos, y sea 1=m.c.d.(a,b). Sea también (x_0,y_0) una solución particular de la ecuación ax+by=n. Entonces:

(x,y) es solución de la ecuación si, y solo si, $\exists t\in\mathbb{Z}$ con $\begin{cases} x = x_0 + tb \\ y = y_0 - ta \end{cases}$

-Dem-

$\Leftarrow$ Si $x=x_0+tb$ e $y=y_0-ta$, entonces:

$ax+by=ax_0+atb+by_0-bta=[(x_0,y_0)$ es solución particular$]=n+t(ab-ba)=n+0=n$.

$\Rightarrow$ Supongamos que ax+by=n. Por otra parte se tiene que $ax_0+by_0=n$, ya que (x_0,y_0) es solución particular. Restando las dos expresiones obtenemos:

$$a(x-x_0)+b(y-y_0)=0, \qquad (*)$$

de donde se deduce que $b|-a(x-x_0)$.

Como m.c.d.(a,b)=1 se tiene que $b|x-x_0$, es decir existe $t\in\mathbb{Z}$ tal que $x-x_0=tb$, con lo que $x=x_0+tb$.

Sustituyendo $x-x_0$ en (*) se obtiene que $atb+b(y-y_0)=0$ con lo que $y=y_0-ta$. ■

A partir de este resultado es claro que basta conocer una solución de la ecuación diofántica lineal con dos incógnitas para conocerlas todas. Uniendo este hecho con las observaciones anteriores, basta conocer una solución de la ecuación ax+by=1 (1=m.c.d.(a,b)).

I.1.C. ALGORITMO PARA ENCONTRAR UNA SOLUCIÓN

Dada la ecuación ax+by=n con 1=m.c.d(a,b), en primer lugar vamos a calcular una solución de ax+by=1. Para ello calculo el m.c.d.(a,b) mediante el algoritmo de Euclides (aunque ya sepamos que vale 1). De cada división efectuada obtengo una identidad. Si voy sustituyendo progresivamente de una expresión a la anterior y así sucesivamente obtengo la solución particular que buscaba. En segundo lugar basta multiplicar esta solución por n, para obtener una solución de ax+by=n.

Ejemplo

Calcular las soluciones de 26x+34y=14.

Antes de nada divido por 2=m.c.d (26,54), obteniendo la ecuación 13x+17y=7. Ahora pretendo hallar una solución de 13x+17y=1. Utilizo el algoritmo de Euclides:

Al dividir 17 entre 13 obtengo: 17=1.13+4

Al dividir 13 entre 4 obtengo: 13=3.4+1

Al dividir 4 entre 1 obtengo: 4=1.4+0

Despejando 4 de la primera expresión y sustituyendo en la segunda obtenemos 13=3(17-13)+1, con lo que 4.13-3.17=1. De esta forma obtengo que (4,13) es una solución particular de 13x+17y=1, con lo que una solución de 13x+17y=7 es (7.4,13.7).

A veces también podemos obtener una solución particular por tanteo. Esto es posible cuando trabajamos con números pequeños. Veámoslo:

Proposición

Sean a,b, y n números enteros. Sean además 1=m.c.d.(a,b). Entonces existe una solución (x_1,y_1) de ax+by=n con $0 \leq y_1 \leq |a|$.

-Dem-

Sea (x_0,y_0) una solución particular cualquiera de la ecuación.

Dividiendo y_0 por a se tiene que existen $t_0, y_1 \in \mathbb{Z}$ tal que $\begin{cases} y_0 = y_1 + t_0 a \\ 0 \leq y_1 < |a| \end{cases}$ con lo que $(x_1,y_1)=(x_0+t_0b,y_0-t_0a)$ es solución ya que como hemos visto es de la forma $(x,y)=(x_0+tb,y_0-ta)$. Además $0 \leq y_1 \leq |a|$. ■

Ejemplo

Para resolver la ecuación 6x+8y=14, la proposición nos asegura que al menos existe una solución con $0 \leq y<3$. Luego bastaría probar con y=0,1,2 para encontrarla.

Observación

Aunque los problemas donde intervienen ecuaciones diofánticas tienen, en general, infinitas soluciones, estas vienen limitadas en ocasiones por datos adicionales del problema, relativos al n1 de cifras de las soluciones, la no negatividad de las soluciones, etc.

I.2. ECUACIONES DIOFÁNTICAS LINEALES CON MÁS DE DOS INCÓGNITAS

Podemos tratar de extender el caso anterior al caso en que hay más de dos incógnitas.

Proposición

La ecuación diofántica $b_1x_1+.....+b_nx_n=m$, donde $b_i,m\in Z$ tiene solución si, y solo si, $m.c.d.(b_1,..,b_n)|m$.

-Dem-

Es similar a la hecha para el caso en que n=2.

Como consecuencia, dividiendo la ecuación por $m.c.d.(b_1,...,b_n)$, obtendremos que la ecuación $a_1x_1+....+a_nx_n=n$, verificando que $m.c.d.(a_1,....,a_n)=1$, es equivalente a $b_1x_1+.....+b_nx_n=m$. Al igual que antes supondremos que los coeficientes de las ecuaciones con las que trabajaremos son primos entre sí. Veamos como calcular las soluciones:

Proposición

Sean $a_1,...,a_n$ números enteros con $m.c.d.(a_1,a_2)=1$. Sea (α,β) una solución de la ecuación $a_1x_1+a_2x_2=1$. Equivalen:

i) $(\alpha_1,.....,\alpha_n)$ es solución de $a_1x_1+....+a_nx_n=n$.

ii) $\exists t\in Z$ con $\begin{cases}\alpha_1=\alpha(n-a_3\alpha_3-....-a_n\alpha_n)+ta_2\\ \alpha_2=\beta(n-a_3\alpha_3-....-a_n\alpha_n)-ta_1\end{cases}$

-Dem-

i)⇒ii) Sea $(\alpha_1,.....,\alpha_n)$ solución. Entonces (α_1,α_2) es solución de $a_1x_1+a_2x_2=n-a_3\alpha_3-....-a_n\alpha_n\in\mathbb{Z}$. Contamos con un resultado que nos garantiza que $\begin{cases}\alpha_1=\alpha(n-a_3\alpha_3-....-a_n\alpha_n)+ta_2\\ \alpha_2=\beta(n-a_3\alpha_3-....-a_n\alpha_n)-ta_1\end{cases}$ (recordemos que $m.c.d.(a_1,a_2)=1$).

ii)⇒i) Basta sustituir:

$$a_1\alpha_1+...+a_n\alpha_n=$$
$$=a_1\left(\alpha\left(n-a_3\alpha_3-.....-a_n\alpha_n\right)+ta_2\right)+a_2\left(\beta\left(n-a_3\alpha_3-...-a_n\alpha_n\right)-ta_1\right)+....+a_n\alpha_n=$$
$$=\left(a_1\alpha+a_2\beta\right)\left(n-a_3\alpha_3-.....-a_n\alpha_n\right)+a_3\alpha_3+....+a_n\alpha_n=[a_1\alpha+a_2\beta=1]=n$$ ■

Ejemplo

Resolver 2x+4y-2z+3u=4

Pasando al segundo miembro las incógnitas y,z se tiene 2x+3u=4-4y+2z. Buscamos una solución de 2x+3u=1. A simple vista obtenemos la solución (x,u)=(-1,1). Multiplicando esta solución por 4-4y+2z, se tiene que (x,u)=(-4+4y-2z,4-4y+2z) es una solución particular de la ecuación. Por la estudiado para dos incógnitas la solución general es (x,u)=(-4+4y-2z+3t,4-4y+2z-2t). Si queremos todas las incógnitas la solución es: (x,y,z,u)=(-4+4y-2z+3t,y,z,4-4y+2z-2t).

Este proceso nos basta para resolver ecuaciones diofánticas lineales en las que hay dos coeficientes primos entre sí. Pero puede ocurrir que todos los coeficientes sean primos entre sí sin que ninguna pareja lo sea. El siguiente resultado nos solventa el problema.

Proposición

Sean $a_1,...,a_n$ números enteros con m.c.d.$(a_1,a_2,...,a_n)=1$. Sean d=m.c.d.$(a_1,...,a_{n-1})$ y $a_i' = \frac{a_i}{d}$ con i=1,....,n-1. Equivalen:

i) $(\alpha_1,.....,\alpha_n)$ es solución de $a_1x_1+....+a_nx_n=n$.

ii) $\exists u \in \mathbb{Z}$ con $\begin{cases} (\alpha_1,....,\alpha_{n-1}) \text{ es solucion de } a_1'x_1+.....+a_{n-1}'x_{n-1}=u \\ \alpha_n \text{ es solucion de } du+a_nx_n=n \end{cases}$

-Dem-

$i) \Rightarrow ii)$

$a_1\alpha_1+....+a_n\alpha_n=n$. Entonces $a_1\alpha_1+...+a_{n-1}\alpha_{n-1}=n-a_n\alpha_n$

Dividiendo por d: $a'_1\alpha_1+...+a'_{n-1}\alpha_{n-1}=\frac{n-a_n\alpha_n}{d}\in\mathbb{Z}$ ya que el primer miembro es entero. Basta tomar $u=\frac{n-a_n\alpha_n}{d}$ para acabar la demostración.

$ii) \Rightarrow i)$

Veamos que $(\alpha_1,.....,\alpha_n)$ es solución de $a_1x_1+....+a_nx_n=n$.

$n=du+a_n\alpha_n=d(a'_1\alpha_1+.....+a'_{n-1}\alpha_{n-1})+a_n\alpha_n=a_1\alpha_1+.....+a_{n-1}\alpha_{n-1}+a_n\alpha_n$ ■

Ejemplo

Resolver la ecuación 6x+10y+15z=8.

Observamos que m.c.d(6,10,15)=1 y que no hay dos coeficientes que sean primos entre sí. Hemos de aplicar el método expuesto en la proposición anterior:

$6x+10y=8-15z \Rightarrow 3x+5y=\frac{8-15z}{2}=u$. Como el primer miembro es entero, también lo será el segundo: $\frac{8-15z}{2}=u \Rightarrow 8-15z=2u \Rightarrow 2u+15z=8$. Resolvemos esta ecuación, donde existe al menos una solución (u,z) con $0 \leq z<2$. Si z=0 se tiene u=4. La solución general de esta ecuación es $\begin{cases} u=4+15t \\ z=-2t \end{cases}$ $t \in \mathbb{Z}$. Sustituyendo u=4+15t en 3x+5y=u tenemos la ecuación 3x+5y=4+15t, donde m.c.d(3,5)=1.

Buscamos una solución de 3x+5y=1. Fácilmente se tiene (x,y)=(2,-1). Multiplicando por 4+15t obtenemos que (x,y)=(8+30t,-4-15t) es una solución de 3x+5y=4+15t.

La solución general de esta ecuación será (x,y)=(8+30t+5s,-4-15t-3s) .

La solución buscada es (x,y,z)=(8+30t+5s,-4-15t-3s,-2t), que depende de los parámetros s y t.

I.3. SISTEMAS DE ECUACIONES DIOFÁNTICAS LINEALES

También podemos estudiar las soluciones de un conjunto de ecuaciones diofánticas lineales. Con lo estudiado hasta ahora acerca de las ecuaciones diofánticas y algún conocimiento sobre resolución de sistemas (regla de Cramer, método de Gauss-Jordan y teorema de Rouché-Frobenius) la resolución de un sistema de ecuaciones diofánticas lineales no debe entrañar dificultad alguna.

Comentar solamente que por el teorema de Rouché-Frobenius un sistema tendrá solución si y solo si el rango de la matriz de coeficientes coincide con el rango de la matriz ampliada. Además una condición necesaria para que halla soluciones enteras es que en cada una de las ecuaciones que componen el sistema el máximo común divisor de los coeficientes que acompañan a las incógnitas divida al término independiente de la ecuación.

Ejemplo

Resolver el sistema de ecuaciones diofánticas $\begin{cases}3x+4y-5z=17\\3x-7y+4z=2\end{cases}$

El rango de la matriz de coeficientes es 2, al igual que el de la ampliada. Elijo x,y como incógnitas principales: $\begin{cases}3x+4y=5z+17\\3x-7y=-4z+2\end{cases}$. Aplicando la regla de Cramer obtenemos que las soluciones (x,y,z) verifican $\begin{cases}11x-9z=15\\33x-19z=127\end{cases}$. (En caso de que en las ecuaciones no se verifique que m.c.d de los coeficientes divide al término independiente la ecuación no tiene soluciones enteras). Veamos como obtengo las soluciones enteras:

Resolvemos la segunda ecuación. Una solución particular es (5,2). La solución completa es (x,z)=(5+19t,2+33t). Sustituyendo en la primera ecuación y desarrollando se obtiene que y=3+27t. La solución es (x,y,z)=(5+19t,3+27t,2+33t)

Nota: En caso de que en el sistema que sale de aplicar Cramer hubiéramos podido despejar las incógnitas de forma que no aparecen cocientes, es decir, por ejemplo si sale $\begin{cases}-6x+2y=10\\9x+3z=3\end{cases}\Leftrightarrow\begin{cases}y=5+3x\\z=1-3x\end{cases}$ todas las soluciones serían enteras y por tanto la solución general es (x,y,z)=(x,5+3x,1-3x)

II. ECUACIONES DIOFÁNTICAS CUADRÁTICAS

En esta sección nos centraremos sólo en el estudio de las ecuaciones diofánticas cuadráticas más importantes. La más importante de todas es la Ecuación de Pell, ya que se puede demostrar que todas las ecuaciones cuadráticas de dos variables ($ax^2+by^2+cxy+dx+ey+f=0$) se pueden reducir a ella. También estudiaremos las ecuaciones pitagóricas.

II.1. ECUACIÓN DE PELL

Diremos que una ecuación cuadrática es de Pell si es de la forma $\mathbf{x^2-dy^2=n}$ donde d y n son números enteros. Al igual que antes sólo nos interesan las soluciones enteras de esta ecuación.

Casos particulares de esta ecuación se conocen desde incluso la época de Arquímedes, en el s. III a.C. Así por ejemplo en el denominado "problema de los bueyes", el cual es un reto a los matemáticos a resolver un sistema de ecuaciones indeterminadas simultaneas en ocho incógnitas, los números de vacas y bueyes de cada uno de cuatro colores diferentes, aparece implicada un caso particular de la ecuación de Pell: $x^2 = 1 + 4729494y^2$.

Este problema necesita de 600 folios para encontrar una solución particular. Es por ello que sólo estudiaremos un caso muy particular en el que d=1.

Estudiemos un caso particular de la ecuación de Pell.

Teorema

La ecuación diofántica $x^2-y^2=n$ tiene solución si y solo si n se puede factorizar como producto de dos números de la misma paridad, es decir ambos pares o ambos impares. Si existen, las soluciones de esta ecuación tienen la forma

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

donde a y b recorren todos los pares de números de la misma paridad y tales que n=ab.

-Dem-

$\Rightarrow$ Podemos escribir n=(x+y)(x-y) donde x-y y x+y tienen la misma paridad, ya que x+y=(x-y)+2y.

$\Leftarrow$ Supongamos que n=ab donde a y b tienen la misma paridad. Si tomo

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

se tiene que $x^2-y^2=n$, o sea (x,y) es solución. (La comprobación es rutinaria) ■

Nota: Si (x,y) es solución también lo serán (-x,y), (x,-y), (-x,-y)

Ejemplo

Encontrar todas las soluciones positivas de la ecuación $x^2-y^2=120$.

Factorizando obtengo $120=2^3.3.5$. Entonces podemos escribir 120 como producto de la misma paridad de las siguientes maneras:

120=60.2=30.4=20.6=12.10=10.12=6.20=4.30=2.60

Basta sustituir en x=(a+b)/2 e y=(a-b)/2 cada combinación de a y b.

II.2. ECUACIÓN PITAGÓRICA

Otra ecuación diofántica muy importarte es la siguiente. Consideremos ahora x,y,z números naturales. Lo que queremos ahora es resolver la ecuación $\mathbf{x^2+y^2=z^2}$, llamada ecuación pitagórica. Este problema es equivalente a encontrar todos los triángulos rectángulos con lados de longitud entera y fue estudiado por los geómetras griegos. Pitágoras encontró una cantidad infinita de soluciones pero fue Euclides en sus Elementos el que dio la solución completa del problema.

Teorema

Sean x,y,z números naturales. Entonces:

$x^2+y^2=z^2$ si, y solo si, existen a,b números naturales primos relativos con distinta paridad y d número natural tal que: $\begin{cases} x = 2abd \\ y = d(a^2-b^2) \\ z = d(a^2+b^2) \end{cases}$ o $\begin{cases} y = 2abd \\ x = d(a^2-b^2) \\ z = d(a^2+b^2) \end{cases}$

-Dem-

$\Rightarrow$ Sea d=m.c.d(x,y), entonces existen X,Y naturales tal que $\begin{cases} x = dX \\ y = dY \end{cases}$.

Sustituyendo obtengo que $z^2=x^2+y^2=d^2X^2+d^2Y^2=d^2(X^2+Y^2)$, con lo que $d^2|z^2$. De esta forma existe un Z natural tal que z=dZ. Sustituyendo en la expresión anterior obtenemos que $Z^2=X^2+Y^2$. Además m.c.d.(X,Y)=1.

Como m.c.d.(X,Y)=1, se tiene que X ó Y es impar. Supongamos que Y es impar (en otro caso, obtendríamos la otra solución). Veamos que X es par.

Si X fuese impar, se tendría que:

X=2k+1, Y=2r+1, por lo que:

$Z^2=(2k+1)^2+(2r+1)^2=(4k^2+4k+1)+(4r^2+4r+1)=4(k^2+k+r^2+1)+2$ lo cual significa que cuadrado Z^2 es par y no es múltiplo de 4, lo cual es contradicción porque todo cuadrado par es múltiplo de 4.

Por tanto como X es par, e Y impar, Z es impar.

Entonces $X^2=Z^2-Y^2=(Z+Y)(Z-Y)$ donde X, Z+Y, Z-Y son pares. Por esto existen naturales u,v,w tal que $\begin{cases} X = 2w \\ Z+Y = 2u \\ Z-Y = 2v \end{cases}$.

Entonces:

$4w^2=X^2=(Z+Y)(Z-Y)=2u2v$, con lo que $w^2=uv$.

$2u+2v=(Z+Y)+(Z-Y)=2Z$, con lo que $u+v=Z$

$2u-2v=(Z+Y)-(Z-Y)=2Y$, con lo que $u-v=Y$

Veamos que u,v son primos entre sí:

Si m.c.d.$(u,v)\neq 1$, entonces $\exists$p natural primo tal que p|u,v de donde se deduce que p|u+v,u-v; entonces p|Z,Y; entonces $p|Z^2-Y^2=X^2$; entonces p|X; entonces p|m.c.d.(X,Y), lo cual es contradicción ya que m.c.d(X,Y)=1.

Como el producto de u por v es un cuadrado, ambos serán cuadrados, es decir existen a,b naturales tal que $u=a^2$, $v=b^2$. Sustituyendo:

$Z=u+v=a^2+b^2$, con lo que $z=dZ=d(a^2+b^2)$

$Y=u-v=a^2-b^2$, con lo que $y=dY=d(a^2-b^2)$

$w^2=uv=a^2b^2$, entonces w=ab, con lo que X=2w==2ab y por tanto x=dX=2abd

Veamos que m.c.d.(a,b)=1.

m.c.d.(u,v)=1, entonces m.c.d.$(a^2,b^2)=1$, con lo que m.c.d.(a,b)=1.

Veamos que a,b tienen distinta paridad. Si fueran ambos pares o ambos impares entonces $Z^2=a^2+b^2$, $Y=a^2-b^2$ serían ambos pares, de donde se deduce que X es par ya que $X^2=Z^2- Y^2$ es par. Entonces 2|m.c.d.(X,Y) lo cual es contradicción. $\boxed{\Leftarrow}$ Basta sustituir las expresiones en la ecuación pitagórica. ■

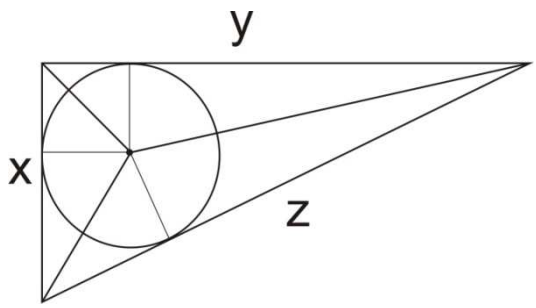
Observación: Obsérvese que este resultado nos permite calcular las soluciones naturales de la ecuación pitagórica. Para obtener las enteras, bastará cambiar el signo de alguna coordenada de la terna solución.

Aplicación

Demostrar que el radio de la circunferencia inscrita en un triángulo pitagórico de lados enteros es siempre un número natural.

-Dem-

Sea r el radio de la circunferencia inscrita y sean x,y,z las longitudes de los lados del triángulo, donde z es la hipotenusa. Entonces $z^2=x^2+y^2$.



El área del triángulo es $\frac{xy}{2}$. Uniendo el centro de la circunferencia inscrita con los tres vértices del triángulo, este que subdividido en tres triángulos cuya suma de áreas es el área del triángulo de partida:

$\frac{1}{2}xy=\frac{1}{2}xr+\frac{1}{2}yr+\frac{1}{2}zr=\frac{1}{2}r(x+y+z)$ con lo que $r=\frac{xy}{x+y+z}$. Por el teorema anterior se la forma de x,y,z. Sustituyendo obtengo que:

$$r=\frac{xy}{x+y+z}=\frac{2abdd(a^2-b^2)}{2abd+d(a^2-b^2)+d(a^2+b^2)}=\frac{db(a^2-b^2)}{a+b}=db(a-b)$$ que es natural. ■

III. ECUACIONES DIOFÁNTICAS POLINÓMICAS

En 1900, Hilbert propuso buscar un algoritmo universal para decidir si una ecuación de la forma $P(x_1,....,x_n)=0$ donde P es un polinomio con coeficientes enteros, tiene soluciones enteras. No se ha demostrado la existencia de un algoritmo como el que buscaba Hilbert, aún limitándonos a polinomios de nueve variables, y parece probable que no exista ni siquiera para polinomios de tres variables.

III.1. RESULTADOS PARA ECUACIONES DIOFÁNTICAS DE DOS VARIABLES

Para casos muy concretos sí puede decidirse si una ecuación diofántica tiene solución o no. Así por ejemplo para el caso de una ecuación polinómica homogénea:

Proposición

Sea $P\in\mathbb{Z}[x,y]$ un polinomio homogéneo de grado r (es decir, $P(tx,ty)=t^rP(x,y)$, y sean $x,y\in\mathbb{Z}$. Entonces (x,y) es solución de la ecuación

P(x,y)=0 si solo si una fracción irreducibe $\frac{p}{q}$ raíz del polinomio P(z,1) y existe $t \in \mathbb{Z}$ con $\begin{cases} x = tp \\ y = tq \end{cases}$

Para el caso en el que el polinomio no es homogéneo, no existen resultados generales que permitan lo que quiero. En cambio cabe destacar algunos resultados para los casos en los que el polinomio es de la forma P(x)+by, y otro para el caso en que es de la forma P(x)-Q(x)y. Enunciémoslos:

- Sean $P \in \mathbb{Z}$ [x], y $b \in \mathbb{Z}$. Entonces, los valores de x para los que la ecuación P(x)+by=0 tiene solución entera son congruentes entre sí módulo b.
- La ecuación P(x)-Q(x)y=0, donde $P,Q \in \mathbb{Z}$ [x] y gr(Q)>0, tiene un número finito de soluciones.

Gráficamente una ecuación diofántica con dos variables es una curva, y resolverla es encontrar los puntos del plano de coordenadas enteras por las que pasa.

III.2. OTRAS ECUACIONES DIOFÁNTICAS

III.2.A. ECUACIÓN DE MORDELL

Ya en los años 20, Mordell descubrió algunos resultados relativos a la ecuación $y^2=x^3+k$, donde k es un entero no nulo. Éstos eran propiedades referentes a cuerdas y tangentes desde ciertos puntos. Sin embargo, creyó que para ciertos valores de k la ecuación tenía infinitas soluciones enteras, lo cual no es cierto.

III.2.B. ÚLTIMO TEOREMA DE FERMAT

Una de las posibles generalizaciones de la ecuación pitagórica es la ecuación $x^n+y^n=z^n$ con n>2.

Evidentemente se tienen soluciones del tipo (x,0,x) , (0,x,x). Y si n es par $(\pm x,0,\pm x),(0,\pm x,x)$. Si n es impar (x,-x,0). Todas estas soluciones se denominan soluciones triviales de la ecuación.

El genial matemático francés Pierre de Fermat anotó en un margen de un libro que conocía una demostración "sencilla y elegante" de que cuando n>2, la

ecuación dada solo tiene soluciones triviales. No se ha podido averiguar si Fermat sabía dicha demostración. A lo largo de los últimos cuatro siglos, algunos de los matemáticos más importantes han dedicado parte de sus esfuerzos a la demostración del resultado, sin conseguirlo. Ha sido en 1993 cuando el matemático inglés Andrew Wiles logró demostrar este teorema, mediante la teoría de formas modulares y curvas elípticas, teoría que desconozco totalmente.

IV. BIBLIOGRAFÍA

■ Anderson I. **First Course in Discrete Mathematics**. Springer-Verlag, 2002

■ Biggs N.L. **Matemática Discreta**. Vicens Vives, 1994

■ Grimaldi R.P. **Matemática discreta y combinatoria**. Addson-Wesley Iberoamericana, 1993

■ Bujalance E. y otros. **Elementos de Matemática Discreta**. Editorial Sanz Torrres, Madrid, 1997