N2

Ecuaciones diofánticas

1. La ecuación lineal con dos incógnitas

Se usa el nombre de *ecuaciones diofánticas* para designar una amplia clase de ecuaciones algebraicas con más de una incógnita y con coeficientes enteros y en las que sólo se buscan sus soluciones enteras, esto es, las formadas exclusivamente por números enteros. El apellido de estas ecuaciones hace honor a Diofanto de Alejandría. De entre ellas, se habla en este epígrafe de las ecuaciones lineales de dos incógnitas.

1.1. La ecuación lineal con dos incógnitas $ax+by=c$: *Dados los números enteros a, b y c, con a y b no nulos, la ecuación diofántica lineal*

$$ax+by=c$$

tiene solución entera si y sólo si $d=\mathrm{mcd}(a,b)$ es un divisor de c. En tal caso, si (x_0,y_0) es una solución particular de esta ecuación, cualquier otra solución (x,y) de la misma está dada por

$$x=x_0+\left(\frac{b}{d}\right)t, \qquad y=y_0-\left(\frac{a}{d}\right)t\,, \qquad (t\in\mathbb{Z})\,\blacksquare$$

Puede no resultar sencillo dar "a simple vista" con una solución particular (x_0,y_0) de la ecuación. El Algoritmo de Euclides facilita un procedimiento para su obtención.

1.2. Determinación de una solución particular de la ecuación lineal: El método clásico de búsqueda de una solución particular de la ecuación $ax+by=c$, en la que $d=\mathrm{mcd}(a,b)$ es divisor de c, comienza determinando dos números enteros x_1 e y_1 tales que $ax_1+by_1=d$, números que existen según la Igualdad de Bezout y que pueden deducirse de la aplicación del Algoritmo de Euclides para el cálculo de $\mathrm{mcd}(a,b)=d$. Una vez identificados, una solución particular de la ecuación será

$$(x_0,y_0)=\left(\frac{c}{d}x_1,\frac{c}{d}y_1\right)$$

1.3. Ejemplo: El diámetro de una moneda de un euro es de 23 mm y el de una moneda de dos euros es de 37 mm. ¿Cuántas monedas de cada clase deben elegirse para que al situarlas tangentes con sus centros alineados alcancen exactamente 1 m de longitud?

SOLUCIÓN: Si se llama x al número de monedas de 1 € e y al número de monedas de dos euros que deben utilizarse, entonces

$$23x + 37y = 1000 \tag{1}$$

Esta ecuación tiene solución por ser 23 y 37 primos relativos. Para obtener una solución particular de la ecuación puede recurrirse al Algoritmo de Euclides para el cálculo del $\text{mcd}\,(23, 37) = 1$:

$$37 = 23 \cdot 1 + 14, \quad 23 = 14 \cdot 1 + 9, \quad 14 = 9 \cdot 1 + 5, \quad 9 = 5 \cdot 1 + 4, \quad 5 = 4 \cdot 1 + 1$$

Escribimos ahora 1 como combinación lineal entera de 23 y 37 razonando de derecha a izquierda en los cálculos anteriores:

$$1 = 5 - 4 = 5 - (9 - 5) = 2 \cdot 5 - 9 = 2 \cdot (14 - 9) - 9 = 2 \cdot 14 - 3 \cdot 9 =$$

$$= 2 \cdot 14 - 3 \cdot (23 - 14) = 5 \cdot 14 - 3 \cdot 23 = 5 \cdot (37 - 23) - 3 \cdot 23 = (-8) \cdot 23 + 5 \cdot 37$$

es decir,

$$(-8) \cdot 23 + 5 \cdot 37 = 1\,.$$

Multiplicando esta relación por 1000, se obtiene:

$$(-8000) \cdot 23 + 5000 \cdot 37 = 1000$$

lo que demuestra que $x_0 = -8000\,,\ y_0 = 5000$ es una solución particular de la ecuación.

Las soluciones de la ecuación (1) son entonces

$$x = -8000 + 37t, \qquad y = 5000 - 23t, \qquad (t \in \mathbb{Z})$$

Como además deben ser $x, y > 0$, t debe ser elegido de modo que $-8000 + 37t > 0$ y $5000 - 23t > 0$, es decir, $t > 216$ y $t < 218$, así que necesariamente $t = 217$, por lo que deben alinearse

$$x = -8000 + 37 \cdot 217 = 29 \text{ monedas de 1 euro}, \qquad y = 5000 - 23 \cdot 217 = 9 \text{ monedas de 2 euros} \blacksquare$$

El teorema 1.1 puede ser extendido a ecuaciones lineales diofánticas de más de dos variables, como establece el resultado siguiente:

1.4. Ecuación lineal de n variables: *Si $a_1, a_2, \ldots, a_n$ son enteros no nulos, la ecuación*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

tiene solución entera si y sólo si $d = \text{mcd}\,(a_1, a_2, \ldots, a_n)$ es un divisor de c. Además, en tal caso, el sistema tiene infinitas soluciones enteras.

Podemos limitarnos a resolver las ecuaciones lineales $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ en las que $\text{mcd}\,(a_1, a_2, \ldots, a_n) = 1$ pues, si no es así, basta dividir todos sus términos por $d = \text{mcd}\,(a_1, a_2, \ldots, a_n)$ y obtener la ecuación equivalente

$$\frac{a_1}{d}\,x_1 + \frac{a_2}{d}\,x_2 + \ldots + \frac{n}{d}\,x_n = \frac{c}{d}\,,$$

en la que $\text{mcd}\,(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}) = 1$.

El siguiente resultado resuelve estas ecuaciones lineales si existen coeficientes a_i y a_j que sean coprimos. Supondremos, por comodidad, que son a_{n-1} y a_n.

1.5. Soluciones de una ecuación lineal con más de dos incógnitas y al menos dos coeficientes primos relativos: *Sea*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$$

una ecuación diofántica lineal en la que $\text{mcd}(a_1, a_2, \ldots, a_n) = 1$ *y* $\text{mcd}(a_{n-1}, a_n) = 1$. *Entonces, la ecuación tiene infinitas soluciones enteras* $(x_1, x_2, \ldots, x_n)$ *y cualquiera de ellas es de la forma*

$$x_1 = t_1, \quad x_2 = t_2, \quad \ldots \quad x_{n-2} = t_{n-2}, \quad x_{n-1} = \alpha(c - a_1t_1 - \ldots - a_{n-2}t_{n-2}) + a_ns, \quad x_n = \beta(c - a_1t_1 - \ldots - a_{n-2}t_{n-2}) - a_{n-1}s, \qquad (t_1, \ldots, t_{n-2}, s \in \mathbb{Z})$$

donde (α, β) *es una solución particular de la ecuación* $a_{n-1}x_{n-1} + a_nx_n = 1$.

1.6. Ejemplo: Resolvemos la ecuación lineal diofántica $2x - 6y + 3z + 12u = 5$.

SOLUCIÓN: Como es $\text{mcd}(2, -6, 3, 12) = 1$, la ecuación tiene solución. Como es $\text{mcd}(2, 3) = 1$, si llamamos $y = r$, $u = s$, donde $r, s \in \mathbb{Z}$, debemos resolver la ecuación con dos incógnitas:

$$2x + 3z = 5 + 6r - 12s \qquad (1)$$

Buscamos para ello una solución particular de $2x + 3z = 1$. Se observa inmediatamente que el par $(-1, 1)$ lo es, por lo que una solución particular de (1) es $(x_0, z_0) = (-5 - 6r + 12s,\ 5 + 6r - 12s)$, y cualquier solución de (1) es de la forma:

$$(x, z) = (-5 - 6r + 12s + 3t, 5 + 6r - 12s - 2t), \qquad t \in \mathbb{Z}$$

Por tanto, las soluciones de la ecuación inicial son las cuaternas (x,y,z,u) tales que

$$(x,y,z,u) = (-5-6r+12s+3t,\ r,\ 5+6r-12s-2t,\ s)\,, \qquad (r,s,t \in \mathbb{Z})\ \blacksquare$$

Cuando se trata de resolver ecuaciones lineales $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ en las que $\operatorname{mcd}(a_1,a_2,\ldots,a_n) = 1$ y, en cambio, $\operatorname{mcd}(a_i,a_j) \neq 1$, para todo $i \neq j$, se utiliza el resultado siguiente:

1.7. Soluciones de una ecuación lineal diofántica con más de dos incógnitas y sin un par de coeficientes primos relativos: *Sea*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$$

una ecuación diofántica lineal en la que $\operatorname{mcd}(a_1,a_2,\ldots,a_n) = 1$, $\operatorname{mcd}(a_i,a_j) \neq 1$ si $i \neq j$, *y sea* $d = \operatorname{mcd}(a_1,\ldots,a_{n-1})$. *Entonces,* $(x_1,x_2,\ldots,x_n)$ *es solución entera de la ecuación si y sólo si* $(\frac{a_1}{d}x_1 + \cdots + \frac{a_{n-1}}{d}x_{n-1}, x_n)$ *es solución entera de la ecuación* $du + a_nx_n = c$, *cuyas incógnitas son* (u, x_n) $\blacksquare$

Según lo anterior, para resolver la ecuación lineal diofántica $a_1x_1 + \cdots + a_nx_n = c$ en la que $n > 2$, se comienza encontrando todas las soluciones (u,x_n) de la ecuación diofántica lineal con dos incógnitas $du + a_nx_n = c$. Una vez obtenidas, todo se reduce a resolver la ecuación lineal de $n-1$ incógnitas $\frac{a_1}{d}x_1 + \ldots + \frac{a_{n-1}}{d}x_{n-1} = u$, en la que $\operatorname{mcd}(\frac{a_1}{d},\ldots,\frac{a_{n-1}}{d}) = 1$. Si esta ecuación cumple las hipótesis de 1.5, se resuelve como allí se indica. De no ser así basta reducirla a una ecuación con $n-2$ incógnitas como se indica en 1.7. Repitiendo sucesivamente este proceso se llega a una ecuación lineal con dos incógnitas con solución conocida.

1.8. Ejemplo: Resolvemos la ecuación diofántica lineal $6x + 10y + 15z = 8$.

SOLUCIÓN: Observamos que $\text{mcd}\,(6,10,15)=1$ y no hay dos coeficientes primos entre sí. Escribimos entonces $6x+10y=8-15z$, es decir, $3x+5y=\frac{8-15z}{2}$. Como el primer miembro es entero, también lo es el segundo y, para algún $u\in\mathbb{Z}$, será $\frac{8-15z}{2}=u$, es decir,

$$2u+15z=8$$

No hay que discurrir mucho para obtener $(u_0,z_0)=(4,0)$ como solución particular de la ecuación anterior, por lo que su solución general es $u=4+15s$, $z=-2s$, con $s\in\mathbb{Z}$. Al sustituir el valor obtenido para u en $3x+5y=u$, debemos resolver la ecuación

$$3x+5y=4+15s \tag{2}$$

Como una solución particular de la ecuación $3x+5y=1$ es, a simple vista, $(2,-1)$, deducimos que $(x_0,y_0)=(2\,(4+15s),-(4+15s))=(8+30s,-4-15s)$ es solución particular de (2), así que cualquier solución entera de (2) es

$$(x,y)=(8+30s+5t,\,-4-15s-3t)\,,$$

donde también $t\in\mathbb{Z}$. Se obtiene así que cualquier solución de la ecuación original es:

$$(x,y,z)=(8+30s+5t,\,-4-15s-3t,\,-2s)\,,\qquad (s,t\in\mathbb{Z})$$

2. Congruencias lineales

La resolución de la ecuación lineal con dos incógnitas implica la resolución de la ecuación en congruencias $ax\equiv b\,(\text{mod}\,n)$, pues ésta tiene solución si y sólo si existe un número $y\in\mathbb{Z}$ tal que $ax=b+ny$, y esto ocurre sólo cuando la ecuación lineal $ax-ny=b$ tiene solución, pero esto equivale a que el máximo común divisor de a y n sea divisor de b. Se ha probado así el siguiente resultado:

2.1. La congruencia lineal $ax \equiv b \pmod{n}$: *Dados los números enteros a y b no simultáneamente nulos, y $n \in \mathbb{N}$, $n \geq 2$, la ecuación en congruencias $ax \equiv b \pmod{n}$ tiene solución si y sólo si $d \mid b$, donde $d = \mathrm{mcd}(a,n)$. En tal caso, si x_0 es una solución particular de dicha ecuación, cualquier solución de la misma es de la forma*

$$x = x_0 + \frac{n}{d}t\,, \qquad (t \in \mathbb{Z}\,) \ \blacksquare$$

El teorema anterior establece que si el máximo común divisor de a y n es un divisor de b y x_0 es una solución particular de la congruencia lineal, entonces las ecuaciones $ax \equiv b \pmod{n}$ y $x \equiv x_0 \pmod{\frac{n}{d}}$ son equivalentes.

2.2. Ejemplo: Resolvemos la ecuación $6x \equiv 9 \pmod{15}$.

SOLUCIÓN: Al ser $\mathrm{mcd}(6,15) = 3$ un divisor de 9, la ecuación tiene solución única módulo $n = \frac{15}{3} = 5$. Para encontrarla, aplicamos las propiedades de las congruencias. El número entero x es solución de la congruencia si y sólo si

$$6x \equiv 9 \pmod{15} \quad \Leftrightarrow \quad 2x \equiv 3 \pmod{5} \quad \Leftrightarrow \quad 2x \equiv 8 \pmod{5} \quad \overset{\mathrm{mcd}(2,5)=1}{\Leftrightarrow} \quad x \equiv 4 \pmod{5}$$

Cualquier solución entera de la ecuación es por tanto de la forma $x = 4 + 5t$, donde $t \in \mathbb{Z}$.

2.3. Ejemplo: Resolvemos la ecuación $9x \equiv 21 \pmod{30}$.

SOLUCIÓN: Como es $\mathrm{mcd}(9,30) = 3$ un divisor de 21, la ecuación tiene solución única módulo $n = \frac{30}{3} = 10$. Dado que

$$9x \equiv 21 (\mathrm{mod}\, 30) \quad \Leftrightarrow \quad 3x \equiv 7 (\mathrm{mod}\, 10) \quad \Leftrightarrow \quad 3x \equiv -3 (\mathrm{mod}\, 10) \overset{\mathrm{mcd}(3,10)=1}{\Leftrightarrow} \quad x \equiv -1 (\mathrm{mod}\, 10)\,,$$

toda solución de la ecuación es de la forma $x = -1 + 10t$, donde $t \in \mathbb{Z}$.

2.4. Corolario: *Si* $\mathrm{mcd}(a,n) = 1$, *la congruencia lineal* $ax \equiv b (\mathrm{mod}\, n)$ *tiene solución única módulo n, es decir, cualquier solución entera de la ecuación es de la forma*

$$x = x_0 + nt\,, \quad (t \in \mathbb{Z}\,) \ \blacksquare$$

Las congruencias lineales proporcionan un método alternativo para obtener las soluciones enteras de una ecuación lineal con dos incógnitas $ax + by = c$, que no requiere del cálculo de una solución particular y tampoco precisa del conocimiento de la fórmula que da su solución general. Utilizamos este procedimiento general para resolver el siguiente problema:

2.5. Ejemplo (Euler, 1776): Se pretenden envasar los 100 litros de vino de un barril en garrafas de 7 litros y 11 litros. ¿Cuántas garrafas de cada tipo serán necesarias para que todas las garrafas queden llenas y no quede vino en el barril?

SOLUCIÓN: Si llamamos x al número de garrafas de 7 litros que se emplean e y al número de garrafas de 11 litros, debe ser:

$$7x + 11y = 100 \tag{2}$$

Para resolver la ecuación lineal anterior, razonamos como sigue: si (x,y) es solución entera de la ecuación. al despejar en ésta el término literal con mayor coeficiente en valor absoluto se tiene, aplicando las propiedades de las congruencias:

$$11y = 100 - 7x \quad \Rightarrow \quad 11y \equiv 100 (\mathrm{mod}\, 7) \quad \Rightarrow \quad 4y \equiv 2 (\mathrm{mod}\, 7) \overset{\mathrm{mcd}(2,7)=1}{\Rightarrow} \quad 2y \equiv 1 (\mathrm{mod}\, 7) \quad \Rightarrow \quad 2y \equiv 8 (\mathrm{mod}\, 7) \overset{\mathrm{mcd}(2,7)=1}{\Rightarrow} \quad y \equiv 4 (\mathrm{mod}\, 7)$$

Por tanto, será $y = 4 + 7t$, para cierto $t \in \mathbb{Z}$. Al sustituir esta expresión en la ecuación (2) se obtiene:

$$7x + 11(4 + 7t) = 100 \quad \Rightarrow \quad 7x = 56 - 7 \cdot 11t \quad \Rightarrow \quad x = 8 - 11t$$

Las soluciones enteras de la ecuación son por tanto los pares

$$(x, y) = (8 - 11t,\ 4 + 7t), \qquad t \in \mathbb{Z}$$

Como son $x, y \geq 0$, elegimos t para que $8 - 11t \geq 0$ y $4 + 7t \geq 0$, es decir, $t \leq 0$ y $t \geq 0$ y, así que necesariamente $t = 0$, por lo que son $x = 8$, $y = 4$, luego deben envasarse 8 garrafas de 7 litros y 4 garrafas de 11 litros ■

3. Teorema chino de los restos

Cuando se trata de resolver un sistema de congruencias lineales

$$a_i x \equiv b_i (\mathrm{mod}\, m_i), \qquad \text{para } i = 1, \ldots, k,$$

en el que $d_i = \mathrm{mcd}(a_i, m_i)$ es un divisor de b_i para cada $i = 1, \ldots, k$ (en caso contrario el sistema no tiene solución), cada congruencia del sistema equivale a una ecuación del tipo $x \equiv c_i (\mathrm{mod}\, n_i)$, donde c_i es solución particular de la congruencia $a_i x \equiv b_i (\mathrm{mod}\, m_i)$ y $n_i = \frac{m_i}{d_i}$. Por tanto, la resolución del sistema anterior se reduce a la del sistema

$$x \equiv c_i (\mathrm{mod}\, n_i), \qquad \text{para } i = 1, \ldots, k,$$

problema que resuelve el llamado *Teorema chino de los restos* cuando los módulos n_i son primos entre sí.

3.1. Teorema chino de los restos: *Si* $n_1, n_2, \ldots, n_k$ *son enteros positivos primos relativos dos a dos, el sistema de congruencias lineales*

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, n_1) \\ x \equiv a_2 (\mathrm{mod}\, n_2) \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv a_k (\mathrm{mod}\, n_k) \end{cases}$$

tiene solución única módulo $n_1 n_2 \cdots n_k$, *es decir, si* x_0 *es una solución particular del sistema, cualquier solución del mismo es de la forma:*

$$x = x_0 + n_1 n_2 \cdots n_k t, \qquad (t \in \mathbb{Z}) \ \blacksquare$$

Una solución particular del sistema puede obtenerse como sigue: Llámese $n = n_1 n_2 \ldots n_k$ y sea N_j, para cada $j = 1, \ldots, k$, el producto

$$N_j = \frac{n}{n_j} = n_1 \ldots n_{j-1} n_{j+1} \ldots n_k$$

Como los n_i son primos dos a dos, es $\mathrm{mcd}\,(N_j, n_j) = 1$, así es que la congruencia lineal $N_j x \equiv 1 (\mathrm{mod}\, n_j)$ tiene solución única módulo n_j; llamémosla x_j. Entonces, como n_i es divisor de N_j para $i \neq j$, resulta que $N_j \equiv 0 (\mathrm{mod}\, n_i)$, y para cada $i = 1, \ldots, k$, ocurre que $a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_k N_k x_k \equiv a_i N_i x_i \equiv a_i \cdot 1 \equiv a_i \,(\mathrm{mod}\, n_i)$, es decir, una solución particular del sistema es por tanto el número entero

$$x_0 = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_k N_k x_k$$

3.2. Ejemplo (Sun Tsu, siglo I): Encuéntrese el menor número natural que, dividido por 3 da como resto 2, dividido por 5 da de resto 3 y, dividido por 7 da de resto 2.

SOLUCIÓN: Debe encontrarse el menor número natural x que es solución del sistema

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Como quiera que 3, 5 y 7 son primos dos a dos, el sistema tiene solución única módulo $n = 3 \cdot 5 \cdot 7 = 105$. Con la notación anterior, tenemos

$$N_1 = \frac{105}{3} = 35, \qquad N_2 = \frac{105}{5} = 21, \qquad N_3 = \frac{105}{7} = 15.$$

Las congruencias lineales $35x \equiv 1 \pmod 3$, $21x \equiv 1 \pmod 5$ y $15x \equiv 1 \pmod 7$ son equivalentes a $2x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 5$ y $x \equiv 1 \pmod 7$, respectivamente, y éstas admiten como soluciones particulares a $x_1 = 2$, $x_2 = 1$ y $x_3 = 1$, así que una solución particular del sistema está dada por

$$x_0 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$$

y como es $233 \equiv 23 \pmod{105}$, cualquier solución del sistema (todas son congruentes módulo 105), está dada por

$$x = 23 + 105t \quad , \quad t \in \mathbb{Z}$$

La menor solución positiva se obtiene para $t = 0$, y no es otra que 23, que es el número que pide el problema ■

El siguiente ejercicio, similar al anterior, muestra un método más sencillo de recordar para resolver sistemas de congruencias lineales.

3.3. Ejemplo: Cierto número natural menor que 1200 da como restos 1, 2 y 6 cuando se divide por 9, 11 y 13, respectivamente. ¿De qué número se trata?

SOLUCIÓN: Se busca un número entero x tal que

$$x \equiv 1 (\mathrm{mod}\, 9), \qquad x \equiv 2 (\mathrm{mod}\, 11), \qquad x \equiv 6 (\mathrm{mod}\, 13). \tag{3}$$

Por ser los módulos 9, 11 y 13 primos relativos dos a dos, el sistema tiene solución única módulo $9 \cdot 11 \cdot 13 = 1287$ según el *Teorema chino de los restos*. Para encontrar dicha solución, podemos razonar así: Si x es solución del sistema, lo es de la primera ecuación, luego será $x = 1 + 9r$, para algún $r \in \mathbb{Z}$. Al sustituir en la segunda, se tiene:

$$1 + 9r \equiv 2 \ (\mathrm{mod}\, 11) \quad \Rightarrow \quad 9r \equiv 1 \ (\mathrm{mod}\, 11) \quad \Rightarrow \quad -2r \equiv 12 \ (\mathrm{mod}\, 11) \overset{\mathrm{mcd}(-2,11)=1}{\Rightarrow} \quad r \equiv -6 \ (\mathrm{mod}\, 11)$$

y por tanto $r = -6 + 11s$, para algún $s \in \mathbb{Z}$, luego será $x = 1 + 9r = 1 + 9(-6 + 11s) = -53 + 99s$. Como x cumple la última congruencia:

$$-53 + 99s \equiv 6 (\mathrm{mod}\, 13) \quad \Rightarrow \quad 99s \equiv 59 (\mathrm{mod}\, 13) \quad \Rightarrow \quad 8s \equiv 7 (\mathrm{mod}\, 13) \quad \Rightarrow \quad -5s \equiv 20 (\mathrm{mod}\, 13) \overset{\mathrm{mcd}(-5,13)=1}{\Rightarrow} \quad s \equiv -4 (\mathrm{mod}\, 13)$$

es decir, será $s = -4 + 13t$, para algún $t \in \mathbb{Z}$, y por tanto, cualquier solución del sistema de congruencias lineales (3) es

$$x = -53 + 99s = -53 + 99(-4 + 13t) = -449 + 1287t\,, \qquad (t \in \mathbb{Z})$$

El único de estos números enteros comprendido entre 1 y 1200 se obtiene para $t = 1$, y es $x = -449 + 1287 = 838$ ■

Cuando se trata de resolver el sistema de congruencias lineales cuyos módulos n_i no son primos relativos dos a dos, es de aplicación el siguiente resultado, que generaliza al *Teorema chino de los restos*.

3.4. Teorema: *Si* $n_1, n_2, \ldots, n_k$ *son enteros positivos mayores que* 1 *y* $a_1, a_2, \ldots, a_k$ *son enteros cualesquiera, el sistema de congruencias lineales*

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, n_1) \\ x \equiv a_2 (\mathrm{mod}\, n_2) \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv a_k (\mathrm{mod}\, n_k) \end{cases}$$

tiene solución si y sólo si $\mathrm{mcd}\,(n_i, n_j)$ *es divisor de* $a_i - a_j$*, para todos los* $i, j = 1, \ldots, n$*,* $i < j$*. En tal caso, el sistema tiene solución única módulo* $\mathrm{mcm}\,(n_1, n_2, \ldots, n_k)$*, es decir, si* x_0 *es una solución particular del sistema, cualquier solución del mismo es de la forma:*

$$x = x_0 + \mathrm{mcm}\,(n_1, n_2, \ldots, n_k)\, t, \qquad (t \in \mathbb{Z}) \ \blacksquare$$

3.5. Ejemplo: Unos padres entregados han comprado entre 100 y 150 caramelos para una fiesta infantil con sus hijos. Al empaquetarlos (los caramelos) de 6 en 6 les han sobrado 3; cuando los empaquetaron de 8 en 8 les sobraron 5, mientras que al embolsarlos de 9 en 9 no les ha sobrado ninguno. ¿Cuántos caramelos han comprado para la fiesta?

SOLUCIÓN: Si x es el número de caramelos comprados, debe ser

$$x \equiv 3 (\mathrm{mod}\, 6), \qquad x \equiv 5 (\mathrm{mod}\, 8), \qquad x \equiv 0 (\mathrm{mod}\, 9) \tag{5}$$

Obsérvese que $\mathrm{mcd}\,(6,8)=2$ es divisor de $5-3=2$, que $\mathrm{mcd}\,(6,9)=3$ es divisor de -3 y que $\mathrm{mcd}\,(8,9)=1$ divide a -5, por lo que el sistema tiene solución única módulo $\mathrm{mcm}\,(6,8,9)=72$. Para encontrar las soluciones del sistema razonamos como en 3.3. De la primera congruencia se sigue que, para algún $r\in\mathbb{Z}$, será $x=3+6r$. Al sustituir en la segunda congruencia, se deduce que

$$3+6r\equiv 5\,(\mathrm{mod}\,8)\quad\Rightarrow\quad 6r\equiv 2\,(\mathrm{mod}\,8)\quad\Rightarrow\quad 3r\equiv 1\,(\mathrm{mod}\,4)\quad\Rightarrow\quad 3r\equiv -3\,(\mathrm{mod}\,4)\quad\Rightarrow\quad r\equiv -1\,(\mathrm{mod}\,4)$$

es decir, será $r=-1+4s$, para algún $s\in\mathbb{Z}$, y por tanto $x=3+6(-1+4s)=-3+24s$. Como este valor es solución de la tercera congruencia,

$$-3+24s\equiv 0\ (\mathrm{mod}\,9)\quad\Rightarrow\quad 24s\equiv 3\,(\mathrm{mod}\,9)\quad\Rightarrow\quad 8s\equiv 1\,(\mathrm{mod}\,3)\quad\Rightarrow\quad -s\equiv 1\,(\mathrm{mod}\,3)\quad\Rightarrow\quad s\equiv -1\,(\mathrm{mod}\,3)$$

luego $s=-1+3t$ para algún $t\in\mathbb{Z}$ y cualquier solución entera del sistema (5) será de la forma

$$x=-3+24\,(-1+3t)=-27+72t,\qquad (t\in\mathbb{Z})$$

Como se compraron entre 100 y 150 caramelos, para algún $t\in\mathbb{Z}$ debe ser $100\le -27+72t\le 150$, es decir, $127\le 72t\le 177$, o bien, $2\le t\le 2$ y por tanto es $t=2$. Se compraron en consecuencia $x=-27+72\cdot 2=117$ caramelos.

3.6. Ejemplo (Yih-hing, siglo VIII): Encuentre el único entero positivo menor que 100 que da como restos 2, 3, 4 y 5 al dividirlo por 3, 4, 5 y 6, respectivamente.

SOLUCIÓN: Se pide un número entero x tal que

$$x\equiv 2\,(\mathrm{mod}\,3),\qquad x\equiv 3\,(\mathrm{mod}\,4),\qquad x\equiv 4\,(\mathrm{mod}\,5),\qquad x\equiv 5\,(\mathrm{mod}\,6)\qquad (6)$$

Si observamos la primera y la última congruencia (en las que los módulos son uno múltiplo del otro), el sistema formado por ambas tiene solución pues $\text{mcd}(3,6)=3$ es divisor de $5-2=3$ y, como es $\text{mcm}(3,6)=6$, dicho sistema es equivalente a la última ecuación $x\equiv 5\,(\text{mod}\,6)$. Resulta así que el sistema inicial es equivalente al formado por las tres últimas ecuaciones, es decir,

$$x\equiv 3\,(\text{mod}\,4),\qquad x\equiv 4\,(\text{mod}\,5),\qquad x\equiv 5\,(\text{mod}\,6) \tag{7}$$

Por ser $\text{mcd}\,(4,5)=1$, $\text{mcd}\,(4,6)=2$ divisor de $5-3=2$ y $\text{mcd}\,(5,6)=1$, el sistema tiene solución única módulo $\text{mcm}\,(4,5,6)=60$. Si x es solución del sistema, lo es de la primera ecuación, luego será $x=3+4r$, donde $r\in\mathbb{Z}$. Al sustituir en la segunda, se obtiene que

$$3+4r\equiv 4\ (\text{mod}\,5)\quad\Rightarrow\quad 4r\equiv 1\ (\text{mod}\,5)\quad\Rightarrow\quad 4r\equiv 16\ (\text{mod}\,5)\quad\overset{\text{mcd}(4,5)=1}{\Rightarrow}\quad r\equiv 4\,(\text{mod}\,5)$$

y por tanto $r=4+5s$, para algún $s\in\mathbb{Z}$, de modo que será $x=3+4r=3+4\,(4+5s)=19+20s$. Como x cumple la última congruencia, será:

$$19+20s\equiv 5\,(\text{mod}\,6)\quad\Rightarrow\quad 20s\equiv -14\,(\text{mod}\,6)\quad\Rightarrow\quad 10s\equiv -7\,(\text{mod}\,3)\quad\Rightarrow\quad s\equiv -1\,(\text{mod}\,3)$$

es decir, será $s=-1+3t$, para algún $t\in\mathbb{Z}$, y por tanto, cualquier solución del sistema de congruencias lineales (7) es

$$x=19+20s=19+20\,(-1+3t)=-1+60t\,,\qquad (t\in\mathbb{Z})$$

El único de estos números enteros entre 0 y 100 se obtiene para $t=1$; se trata del número $x=59$ ■

4. La ecuación pitagórica

4.1. La ecuación pitagórica $x^2+y^2=z^2$: *Todas las soluciones* (x,y,z) *de la ecuación* $x^2+y^2=z^2$ *formadas por enteros positivos tales que* $\operatorname{mcd}(x,y,z)=1$, *vienen dadas por la fórmula*

$$x=2st\,,\qquad y=s^2-t^2\,,\qquad z=s^2+t^2$$

o la que resulta de permutar sus dos primeras componentes, donde s *y* t *son enteros de distinta paridad con* $s>t>0$ *y* $\operatorname{mcd}(s,t)=1$.

4.2. Observaciones

1. Del teorema se desprende que toda solución (x,y,z) formada por enteros positivos de la ecuación pitagórica $x^2+y^2=z^2$ es de la forma:

$$x=2kst\,,\qquad y=k(s^2-t^2)\,,\qquad z=k(s^2+t^2)$$

   o la que resulta de permutar sus dos primeras componentes, donde $k,s,t\in\mathbb{Z}^+$, s y t de distinta paridad, $s>t$ y $\operatorname{mcd}(s,t)=1$.

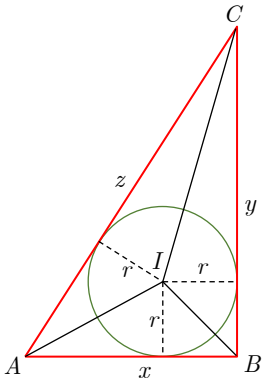
2. Todas las soluciones (x,y,z) de la ecuación pitagórica formadas por números enteros cualesquiera son así, además de las anteriores, las que se obtienen a partir de ellas cambiando el signo de cualquiera de las incógnitas x, y, z y aquéllas en las que alguna de las tres incógnitas es nula, es decir, las $(0,a,\pm a)$ y las $(a,0,\pm a)$, donde $a\in\mathbb{Z}$.

3. Las primeras *ternas pitagóricas primitivas*, esto es, las primeras soluciones (x,y,z), con $x,y,z\in\mathbb{Z}^+$, de la ecuación pitagórica tales que $\operatorname{mcd}(x,y,z)=1$, son las que figuran en la tabla adjunta.

s	t	$x=2st$	$y=s^2-t^2$	$z=s^2+t^2$
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41

4.3. Triángulos pitagóricos: Se llaman *triángulos pitagóricos* a los triángulos rectángulos cuyos lados tienen longitudes enteras. Aplicamos el teorema anterior para demostrar el siguiente curioso resultado sobre la circunferencia inscrita en cualquiera de estos triángulos

4.4. Ejemplo: Demuestre que el radio de la circunferencia inscrita en cualquier triángulo pitagórico es siempre un número entero. ¿Lo es el radio de la circunferencia circunscrita al triángulo?



SOLUCIÓN: Si se une el centro I de la circunferencia inscrita con los tres vértices A, B y C del triángulo, éste queda subdividido en tres triángulos cuya suma de áreas es el área del triángulo ABC, es decir, si r es el radio de la circunferencia inscrita,

$$\frac{1}{2}xy = \frac{1}{2}xr + \frac{1}{2}yr + \frac{1}{2}zr \quad \Rightarrow \quad \frac{1}{2}xy = \frac{1}{2}r(x+y+z) \quad \Rightarrow \quad r = \frac{xy}{x+y+z}$$

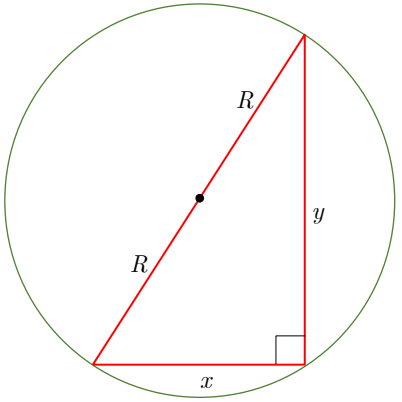
Dado que es $x^2 + y^2 = z^2$, según el teorema anterior serán (suponiendo, por ejemplo, x par):

$$x = 2kst\,, \qquad y = k(s^2 - t^2)\,, \qquad z = k(s^2 + t^2)$$

para ciertos enteros positivos k, s y t tales que $s > t$. Llevando estos valores a la fórmula deducida para r, resulta que el radio de la circunferencia inscrita es

$$r = \frac{2kst \cdot k \cdot (s^2 - t^2)}{2kst + k(s^2 - t^2) + k(s^2 + t^2)} = \frac{2k^2st \cdot (s^2 - t^2)}{2ks(s+t)} = kt(s-t)\,,$$

que es un número entero positivo.



Es conocido que un ángulo α inscrito en una circunferencia abarca sobre ella un arco de amplitud 2α. Es por ello que el ángulo recto de un triángulo rectángulo abarca un arco de $2 \cdot \frac{\pi}{2} = \pi$ radianes sobre su circunferencia circunscrita, pero esto es tanto como decir que la hipotenusa del triángulo es un diámetro de dicha circunferencia. El radio R de la circunferencia circunscrita a un triángulo rectángulo es por tanto la mitad de la longitud de la hipotenusa del triángulo. Deducimos así que si el triángulo rectángulo es pitagórico, R será un número entero si y sólo si la longitud de la hipotenusa es par.

4.5. Último Teorema de Fermat: *Si n es un número entero mayor que 2, la ecuación diofántica*

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

no tiene soluciones enteras positivas.

Fermat dijo tener una "demostración maravillosa" de este resultado, pero no lo bastante breve para contenerla en el estrecho margen de la *Aritmética* de Diofanto. Fermat murió poco después pero nunca se encontró tal demostración y todos los intentos realizados en los tres siglos siguientes a la muerte de Fermat, buscando una demostración de la veracidad de la conjetura o un caso particular que lo contradijera, resultaron fallidos.

A mediados de los años 80 del siglo XX, Faltings probó que el conjunto de soluciones de la ecuación es finito, y en los 90, y tras un primer intento fallido, Andrew Wiles y Richard Taylor presentaron ante la comunidad matemática una demostración definitiva de la Conjetura apoyada en la teoría de curvas elípticas y formas modulares.

5. La ecuación de Fermat

5.1. La ecuación $x^2 - y^2 = n$: *Sea $n \in \mathbb{N}$. La ecuación diofántica $x^2 - y^2 = n$ tiene solución entera si y sólo si n se puede factorizar como producto de dos números enteros de la misma paridad, es decir, ambos pares o ambos impares. En tal caso, las soluciones enteras de la ecuación son:*

$$x = \frac{s+t}{2}, \qquad y = \frac{s-t}{2}$$

donde s y t recorren todos los pares de enteros de igual paridad tales que $n = st$.

5.2. Ejemplo: Exprese si es posible el número $8n^2 + 10n + 3$, donde n es un número entero, como diferencia de dos cuadrados.

SOLUCIÓN: Como $8n^2 + 10n + 3 = (4n+3)(2n+1)$ es el producto de dos números impares, puede ser expresado como diferencia de dos cuadrados. En concreto,

$$8n^2 + 10n + 3 = (4n+3)(2n+1) = \left(\frac{4n+3+2n+1}{2}\right)^2 - \left(\frac{4n+3-2n-1}{2}\right)^2 = (3n+2)^2 - (n+1)^2$$

5.3. Observaciones

1. El teorema anterior establece que un número natural n puede expresarse como la diferencia de dos cuadrados si y sólo si n es el producto de dos números enteros de la misma paridad. En particular, si n es la diferencia de dos cuadrados, n es impar o es múltiplo de 4, pues si n es el producto de dos números impares, n será impar, mientras que si es el producto de dos números pares, n será múltiplo de 4.

2. La obtención de las soluciones, cuando existen, de la ecuación de Fermat $x^2 - y^2 = n$ puede simplificarse atendiendo a la paridad de n como sigue:

   - Si n es impar, s y t deben ser impares para que la ecuación tenga solución, así es que se determinan todos los pares ordenados (s,t) de números enteros impares tales que $st = n$ y a partir de ellos las soluciones (x,y).

   - Si n es par, s o t deben ser pares, y por tanto, para que la ecuación tenga solución deben serlo ambos. Es así que si n no es múltiplo de 4, la ecuación no tiene solución, mientras que si n es múltiplo de 4, los cálculos se facilitan poniendo $n = 4n_1$, $s = 2s_1$, $t = 2t_1$, con lo que $s_1 \cdot t_1 = n_1$ y las soluciones son $x = s_1 + t_1$, $y = s_1 - t_1$.

5.4. Ejemplos: Resolvemos en $\mathbb{Z}$ las ecuaciones:

- $x^2 - y^2 = 9$

  Las parejas de números impares cuyo producto es 9 son los que figuran en la tabla adjunta. La ecuación tiene por tanto seis soluciones.

s	t	$x = \frac{s+t}{2}$	$y = \frac{s-t}{2}$
1	9	5	-4
-1	-9	-5	4
3	3	3	0
-3	-3	-3	0
9	1	5	4
-9	-1	-5	-4

- $x^2 - y^2 = 14$

  Por ser 14 par, pero no múltiplo de 4, la ecuación no tiene solución.

- $x^2 - y^2 = 12$

  Por ser $12 = 4 \cdot 3$, se determinan los pares de números enteros s_1 y t_1 cuyo producto es 3.

s_1	t_1	$x = s_1 + t_1$	$y = s_1 - t_1$
1	3	4	-2
-1	-3	-4	2
3	1	4	2
-3	-1	-4	-2

6. Algunas ecuaciones diofánticas polinómicas

6.1. Ecuaciones $P(x) = Q(x) \cdot y$: *Dados* $P(x), Q(x) \in \mathbb{Z}[x]$, *con* $\operatorname{grad} Q \geq 1$, *la ecuación* $P(x) = Q(x)y$ *tiene un número finito de soluciones enteras* (x, y).

DEMOSTRACIÓN: Para encontrar dichas soluciones despéjese $y = \dfrac{P(x)}{Q(x)}$ y efectúese la división euclídea, obteniendo $c(x)$, $r(x) \in \mathbb{Q}[x]$, con $\operatorname{grad}(r) < \operatorname{grad}(Q)$, tales que

$$P(x) = Q(x) \cdot c(x) + r(x)$$

Si m es el mínimo común múltiplo de todos los denominadores que aparecen en los coeficientes de $c(x)$ y $r(x)$, tenemos que

$$C(x) = m \cdot c(x) \qquad \text{y} \qquad R(x) = m \cdot r(x)$$

son polinomios con coeficientes enteros y además

$$m \cdot P(x) = Q(x) \cdot C(x) + R(x),$$

luego

$$m \cdot y = m \cdot \frac{P(x)}{Q(x)} = \frac{Q(x) \cdot C(x) + R(x)}{Q(x)} = C(x) + \frac{R(x)}{Q(x)} \quad \Rightarrow \quad m \cdot y - C(x) = \frac{R(x)}{Q(x)}$$

Si (x, y) es solución entera de la ecuación, my y $C(x)$ son enteros y por tanto también debe serlo $\dfrac{R(x)}{Q(x)}$, condición que sólo cumple una cantidad finita de números enteros x.

6.2. Ejemplo: Los lados de un rectángulo vienen dados por números enteros positivos. ¿Cuál será la longitud de dichos lados para que el perímetro y la superficie de dicha figura se expresen con el mismo número?

Este problema figura resuelto en la página 714 del volumen 2 de Problemas de Oposiciones de Editorial Deimos.

SOLUCIÓN: Si se llaman x e y a las longitudes de los lados del rectángulo, x e y son enteros positivos y, además

$$xy = 2x + 2y$$

Despejamos una de las dos incógnitas en función de la otra. Se obtiene así:

$$y\,(x-2) = 2x$$

y por tanto

$$y = \frac{2x}{x-2} = \frac{2x-4+4}{x-2} = 2 + \frac{4}{x-2} \quad \Rightarrow \quad y - 2 = \frac{4}{x-2}$$

La última igualdad dice que $x-2$ debe ser divisor de 4, es decir,

$$x-2 = \pm 1\,, \qquad x-2 = \pm 2 \qquad \text{o} \qquad x-2 = \pm 4\,.$$

Las seis ecuaciones sólo dan como valores admisibles $x = 1$, $x = 3$, $x = 4$ o $x = 6$, y de ellos tampoco es válido $x = 1$, pues da $y = -2$. Las únicas soluciones del problema son

$$(x, y) = (3, 6)\,, \qquad (x, y) = (4, 4)\,, \qquad (x, y) = (6, 3)\,.$$

6.3. Ecuaciones $P(x)=my$: *Dados el polinomio* $P(x)\in\mathbb{Z}[x]$ y $m\in\mathbb{Z}$, *las soluciones de la ecuación* $P(x)=my$ *son los* (x,y) *tales que*

$$x=x_0+mt\,,\qquad P(x_0+mt)=my$$

donde $x_0\in\{0,1,2,\ldots,m-1\}$ *es solución particular de la ecuación* $P(x)\equiv 0\,(\mathrm{mod}\,m)$.

Según esta proposición, para resolver la ecuación diofántica $P(x)=my$ basta resolver la ecuación $P(x)\equiv 0\,(\mathrm{mod}\,m)$. Las soluciones de esta ecuación son los $x=x_0+mt$, donde $x_0\in\{0,1,\ldots,m-1\}$ es una solución particular de la misma (si es que existe). Los correspondientes valores de y se obtienen sustituyendo en la ecuación original.

6.4. Ejemplo: Resolvemos la ecuación diofántica $x^2+5x+4+6y=0$.

$$x^2+5x+4+6y=0\quad\Leftrightarrow\quad x^2+5x+4=-6y\quad\Leftrightarrow\quad x^2+5x+4\equiv 0\,(\mathrm{mod}\,6)\qquad(8)$$

SOLUCIÓN: Los únicos enteros $x\in\{0,1,2,3,4,5\}$ que cumplen la ecuación (3) son $x=2$ y $x=5$, por lo que las soluciones de (8) son los $x=2+6t$ junto con los $x=5+6t$, con $t\in\mathbb{Z}$. Sustituyendo estos valores en la ecuación diofántica, se obtienen los correspondientes valores de y, así es que las soluciones de la ecuación son:

$$\begin{cases}x=2+6t\\ y=-6t^2-9t-3\end{cases}\quad,\quad\begin{cases}x=5+6t\\ y=-6t^2-15t-9\end{cases}\qquad(t\in\mathbb{Z})$$

6.5. Ecuaciones polinómicas homogéneas $P(x,y)=0$: *Sea $P(x,y)$ un polinomio con coeficientes enteros y homogéneo, esto es, con todos sus términos del mismo grado no nulo. Entonces, las soluciones enteras de la ecuación $P(x,y)=0$ tales que $y\neq 0$ son los pares (x,y) tales que*

$$x=pt,\quad y=qt \qquad (t\in\mathbb{Z},\ t\neq 0\ )$$

donde $\frac{p}{q}$ $(p\in\mathbb{Z},\ q\in\mathbb{N})$ es cada fracción irreducible solución de la ecuación $P(z,1)=0$.

6.6. Observaciones: El teorema establece que la ecuación homogénea $P(x,y)=0$ tiene solución entera $(x,y)\in\mathbb{Z}^2$ con $y\neq 0$ si, y sólo si, la ecuación polinómica $P(z,1)=0$ tiene alguna solución racional. Nada se dice sobre la posible existencia de soluciones de la ecuación en las que $y=0$. Por ello, en el estudio particular de cada ecuación habrá que calcular $P(x,0)$ y comprobar si es nulo para algún valor.

6.7. Ejemplo: Resolvemos la ecuación $2x^3+3x^2y-3xy^2-2y^3=0$.

SOLUCIÓN: El polinomio $P(x,y)=2x^3+3x^2y-3xy^2-2y^3$ tiene todos sus términos del mismo grado, por lo que es homogéneo. La ecuación $P(z,1)=0$ es $2z^3+3z^2-3z-2=0$, y tiene por soluciones $z=1$, $z=-2$ y $z=-\frac{1}{2}$. Por tanto, las soluciones enteras (x,y), $y\neq 0$, de la ecuación son:

$$\begin{cases} x=t \\ y=t \end{cases}, \qquad \begin{cases} x=-2t \\ y=t \end{cases}, \qquad \begin{cases} x=-t \\ y=2t \end{cases} \qquad (t\in\mathbb{Z},\ t\neq 0)$$

Si algún par $(x,0)$ fuese solución, sería $P(x,0)=2x^3=0$, es decir, $x=0$, y también es válida la solución nula $(0,0)$, que puede englobarse en las anteriores admitiendo $t=0$.

6.8. Ecuaciones $a^2x^2+bx+c=y^2$: *Si a, b, $c\in\mathbb{Z}$ no son simultáneamente nulos, la ecuación*

$$a^2x^2+bx+c=y^2$$

tiene un número finito de soluciones enteras (x,y) .

DEMOSTRACIÓN: El cambio de variable $z=y-ax$, es decir, $y=ax+z$, reduce la ecuación a una del tipo del epígrafe 4.6, por lo que tiene un número finito de soluciones.

$$a^2x^2+bx+c=(ax+z)^2 \quad\Leftrightarrow\quad a^2x^2+bx+c=a^2x^2+2axz+z^2 \quad\Leftrightarrow\quad z^2+2axz-bx-c=0 \quad\Leftrightarrow\quad (z^2-c)+(2az-b)\,x=0$$

6.9. Ejemplo: Resolvemos la ecuación diofántica $4x^2+3x+3=y^2$.

SOLUCIÓN: Al cambiar $y=2x+z$, la ecuación queda:

$$4x^2+3x+3=(2x+z)^2 \quad\Leftrightarrow\quad 4x^2+3x+3=4x^2+4xz+z^2 \quad\Leftrightarrow\quad 4xz+z^2-3x-3=0 \quad\Leftrightarrow\quad x\,(4z-3)=3-z^2 \quad\Leftrightarrow\quad x=\frac{3-z^2}{4z-3}$$

Efectuando la división euclídea:

$$x=-\frac{1}{4}z-\frac{3}{16}+\frac{39}{16(4z-3)} \quad\Rightarrow\quad 16x=-4z-3+\frac{39}{4z-3}$$

de donde se deduce que $4z-3$ debe ser un divisor de $39=3\cdot13$. Por tanto, $4z-3\in\{\pm1,\pm3,\pm13,\pm39\}$ y los únicos valores enteros de z que verifican lo anterior son $z=1,0,4,-9$. Sustituyendo se obtienen las soluciones respectivas:

$$(x,y)=(2,5),\qquad (x,y)=(-1,-2),\qquad (x,y)=(-1,2),\qquad (x,y)=(2,-5).$$