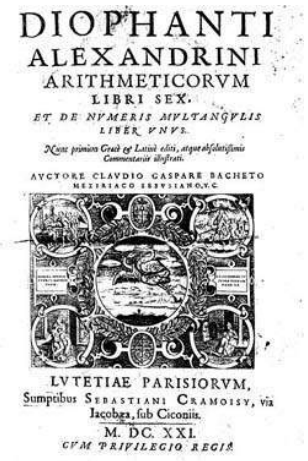
Acerca de las Ecuaciones Diofánticas Lineales

Carlos S. Chinea

0. Introducción


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque obsequiis
Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V. C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via
Jacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS

Las ecuaciones diofánticas, que aparecen por vez primera en uno de los volúmenes de la *Aritmética* de Diofanto de Alejandría, como colección de ejemplos y problemas con valores enteros, tienen cierta utilidad en diversos problemas de la matemática, en donde tanto las variables como las soluciones han de ser números enteros.

Entre las ecuaciones diofánticas más famosas se encuentran las pitagóricas, expresiones en tres variables de la forma $x^2 + y^2 - z^2 = 0$, o la generalización conocida como el *Último Teorema de Fermat,* $x^n + y^n - z^n = 0$, con n natural.

Sin embargo, y aún cuando es de enorme interés su estudio, nos vamos a referir aquí solamente a las ecuaciones diofánticas lineales, esto es, a ecuaciones con coeficientes y soluciones que son números enteros, de la forma

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = c$$

Nos planteamos como objetivo básico establecer tanto condiciones de resolución como algún procedimiento para resolverlas. Para ello trataremos en primer lugar las ecuaciones diofánticas lineales con dos incógnitas para, a continuación, estudiar brevemente las congruencias lineales y aplicarlas a la resolución de ecuaciones diofánticas lineales con mayor número de incógnitas.

1. Ecuaciones Diofánticas Lineales con dos incognitas

Se denominan ecuaciones diofánticas lineales a ecuaciones lineales con coeficientes enteros y cuyas soluciones, de existir, son también números enteros. Es decir, se trata de expresiones de la forma

$$a_1 . x_2 + \ldots + a_n . x_n = c, \qquad a, b, c \in Z$$

Veamos a continuación el caso de las ecuaciones diofánticas lineales con dos incógnitas, esto es, de la forma $ax + by = c$, analizando la existencia de soluciones y el modo de resolución.

Para estudiarlas, establezcamos alguna forma de caracterizar la resolución, esto es de encontrar alguna condición que permita decidir cuando hay o no solución. Para ello veamos el sencillo teorema que sigue, generalizable a ecuaciones de este tipo con cualquier número de incógnitas.

Teorema 1: La condición necesaria y suficiente para que la ecuación diofántica lineal de dos incógnitas $ax + by = c$ tenga solución es que el Máximo Común Divisor de los coeficientes, $d = MCD(a,b)$ divida al término independiente c.

En efecto:

a) Supongamos que hay solución y sea $d = MCD(a,b)$. Veamos que entonces ha de dividir a c:

$$\exists a', b' \in Z / a = d.a', b = d.b' \rightarrow d.a'.x + d.b'.y = c \rightarrow d(a'.x + b'.y) = c \rightarrow d \mid c$$

b) Supongamos que $d = MCD(a,b)$ divide a c. Veamos que entonces hay solución:

$d \mid c \Rightarrow \exists c' \in Z / c = c'.d$. Por otra parte $a = a'.d, b = b'.d$, por lo cual, al sustituir:

$$a.x + b.y = c \rightarrow d.(a'x + b'y) = d.c' \rightarrow a'.x + b'.y = c' \ \wedge MCD(a', b') = 1$$

por la igualdad de Bezout, siempre existen enteros x', y' tales que $a'.x' + b'.y' = 1$, por lo cual:

$$(a'.x' + b'.y').d = d \rightarrow (d.a').x' + (d.b').y' = d \rightarrow a.x' + b.y' = d \rightarrow a.(x'c') + b(y'c') = d.c' \rightarrow$$
$$\rightarrow a.x + b.y = c$$

Por tanto, los enteros x', y' verificarían la ecuación. Son una solución particular de la ecuación diofántica dada.

Este teorema se extiende trivialmente a ecuaciones diofánticas lineales de cualquier número finito de variables: $a_1.x_1 + \ldots + a_n.x_n = c$

Nos preguntamos ahora cómo obtener el conjunto de todas las soluciones de la ecuación diofántica cuando se conoce solamente una solución particular de la misma, es decir, se trata de encontrar cómo están relacionadas estas soluciones. Lo dilucidaremos mediante el teorema siguiente.

Teorema 2: Si es $d = MCD(a,b)$, $d \mid c$. Sean x_0, y_0 una solución particular de la ecuación diofántica lineal $ax + by = c$. Entonces, toda solución, x, y, viene dada por las expresiones:

$$x = x_0 + \frac{b}{d}t \qquad y = y_0 - \frac{a}{d}t$$

donde t es entero $(t \in Z)$.

Demostración:

Veamos, por una parte, que las expresiones anteriores son, realmente, soluciones de la ecuación diofántica, y, por otra, que son todas las soluciones posibles para la ecuación:

- son soluciones. Pues al sustituir:

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

- Son todas las soluciones:

Sea x, y una solución cualquiera de la ecuación. Se tendrá:

$$\begin{cases} a.x + b.y = & c \\ a.x_0 + b.y_0 = & c \end{cases}$$

restando:

$$a.(x - x_0) + b.(y - y_0) = 0 \rightarrow a.(x - x_0) = b.(y_0 - y) \rightarrow \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$$

como $d = MCD(a,b)$, será $MCD\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, de donde, al ser primos entre sí, tendrá que suceder que a/d divide a $(y_0 - y)$ y b/d divide a $(x - x_0)$:

$$\frac{y_0 - y}{a/d} = t \quad \text{y} \quad \frac{x - x_0}{b/d} = t, \text{ con lo que } x = x_0 + \frac{b}{d}t \qquad y = y_0 - \frac{a}{d}t$$

Así pues, cualquier solución x, y se expresa de la forma antedicha.

El problema, pues, de resolver una ecuación diofantica lineal con dos incógnitas se reduce a encontrar una solución particular de la misma. Hay diferentes métodos de hacerlo: mediante "ensayo y error", por el denominado método de Euler, o bien usando el algoritmo de Euclides, o utilizando el algoritmo de la fracciones continuas, etc.. Veamos el método de Euler.

Método de Euler:

Supongamos que queremos encontrar una solución particular de la ecuación diofantica lineal en dos variables $ax + by = c$. Sea $a \leq b$ (si fuera al revés, bastaría intercambiar los papeles de x e y). Descomponemos b y c dividiendo cada uno de estos términos por a: $c = C.a + C_1$ y $b = B.a + B_1$. Y sustituimos en la expresión de la ecuación al despejar la variable x:

$$x = \frac{c - b.y}{a} = C - By + \frac{C_1 - B_1 y}{a}$$

Como $x \in Z$, también $\frac{C_1 - B_1 y}{a} \in Z$ por lo que bastaría ir dando a y los valores $0,1,\ldots,(a-1)$ para encontrar una solución particular y_0, y, sustituyendo en la expresión anterior, de x_0. Esto ha de ocurrir así debido a que el resto de la división $\frac{C_1 - B_1 y}{a}$ ha de ser menor que el divisor a. A lo sumo, $a-1$.

Ejemplos:

1) Encontrar las soluciones de la ecuación diofántica $2x + 7y = 3$, hallando previamente una solución particular.

   Hacemos la descomposición del termino independiente, 3, y del coeficiente mayor, 7, dividiendo cada uno de ellos por el coeficiente 2: 3=1.2+1, 7=3.2+1, con lo que, al sustituir:

$$x = \frac{3 - 7y}{2} = \frac{2 + 1 - (3.2 + 1)y}{2} = 1 - 3y + \frac{1 - y}{2}$$

   Probamos valores para y:

   $y = 1 \rightarrow \frac{1 - 1.1}{2} = 0 \in Z \;\; valido \rightarrow y_0 = 1$. Hallamos x_0: $x_0 = 1 - 3.1 + 0 = -2$

   Solución particular: $(x_0, y_0) = (-2,1)$

   Solución general: $x = x_0 + \frac{b}{d}t = -2 + \frac{7}{1}t = -2 + 7t, \quad y = y_0 - \frac{a}{d}t = 1 - 2t$

   Por tanto: $(x, y) = (-2 + 7t, 1 - 2t), \quad \forall t \in Z$

   Comprobamos la solución general sustituyendo en la ecuación diofántica:

   $2x + 7y = 2.(-2 + 7t) + 7(1 - 2t) = -4 + 14t + 7 - 14t = 3$

2) Encontrar las soluciones de la ecuación diofántica $3x - 5y = 2$.

   Descomponemos ahora los términos 2 y -5: 2=1.3-1, -5=-2.3+1, con lo que

$$x = \frac{2 + 5y}{3} = \frac{3 - 1 + (2.3 - 1)y}{3} = 1 + 2y + \frac{-1 - 1.y}{3}$$

   Probamos valores para y:

   $y = 0 \rightarrow \frac{-1 - 1.0}{3} = -\frac{1}{3} \notin Z \; no \; valido$

   $y = 1 \rightarrow \frac{-1 - 1.1}{3} = -\frac{2}{3} \notin Z \; no \; valido$

   $y = 2 \rightarrow \frac{-1 - 1.2}{3} = -1 \in Z \;\; valido \rightarrow y_0 = 2$. Hallamos x_0: $x_0 = 1 + 2.2 - 1 = 4$

   Solución particular: $(x_0, y_0) = (4,2)$

   Solución general:

$$x = x_0 + \frac{b}{d}t = 4 + \frac{-5}{1}t = 4 - 5t, \quad y = y_0 - \frac{a}{2}t = 2 - \frac{3}{1}t = 2 - 3t$$

Por tanto: $(x, y) = (4 - 5t, 2 - 3t), \quad \forall t \in Z$

Comprobamos esta solución sustituyendo en la ecuación diofántica:

$$3x - 5y = 3.(4 - 5t) - 5(2 - 3t) = 12 - 15t - 10 + 15t = 2$$

En definitiva, resolver una ecuación diofántica lineal en dos variables es muy simple, actuando siempre del mismo modo, esto es, encontrando una solución particular mediante el Método de Euler, y, a continuación, el conjunto infinito de las soluciones mediante las fórmulas obtenidas en el teorema 2.

Sin embargo, se trata ahora de estudiar la resolución de ecuaciones diofánticas lineales de mayor número de variables y de momento, lo único que podemos afirmar de estas ecuaciones es el enunciado del teorema 1, o sea, que es condición necesaria y suficiente que el Máximo Común Divisor de los coeficientes divida al término independiente de la ecuación.

Para estudiar ecuaciones diofánticas lineales de un mayor número de variables debemos utilizar otros procedimientos. En particular podemos ver la utilización de las congruencias lineales. Hacemos, pues, a continuación un resumen expositivo de la teoría de las congruencias lineales a fin de aplicarla luego a la resolución de estas ecuaciones.

2. Una introducción a las congruencias lineales:

2.1. Congruencias:

Dos enteros, a y b, son congruentes modulo m sii dan el mismo resto cuando se dividen por m . Se acostumbra a simbolizar por

$$a \equiv b(\mathrm{mod}\, m)$$

Así, por ejemplo, los números *5* y *9* son congruentes módulo *2,* pues al dividir cada uno de ellos por el *2*, se obtiene el igual resto, 1. Indicaremos, pues: $5 \equiv 9(\mathrm{mod}\, 2)$.

Teorema 3: Se tienen las propiedades inmediatas siguientes:

1. $a \equiv b(\mathrm{mod}\, m) \leftrightarrow \exists k \in Z / a - b = k.m$, o sea, es equivalente que dos números enteros sean congruentes módulo m y que su diferencia sea un múltiplo de m. Si representamos al conjunto infinito de los múltiplos de m por *(m)*, podemos escribir la propiedad así: $a \equiv b(\mathrm{mod}\, m) \leftrightarrow a - b \in (m).$

2. $a \equiv b(\mathrm{mod}\, m) \wedge MCD(a, m) = 1 \rightarrow MCD(b, m) = 1.$ O sea, si dos números son congruentes modulo m, y m es primo con uno de ellos, entonces m es primo con el otro.

3. $a \equiv b(\text{mod } m) \rightarrow (q_0 + q_1^n a) \equiv (q_0 + q_1^n b)(\text{mod } m), \forall q_0, q_1 \in Z.$ Si dos números enteros son congruentes módulo m, también son congruentes modulo m si se les multiplica por una misma potencia natural de un entero q_1 y se les suma un mismo entero q_0.

4. $a \equiv b(\text{mod } m) \wedge f(x) = q_0 + q_1 x + ... + q_n x^n \rightarrow f(a) \equiv f(b)(\text{mod } m)$. Esta propiedad generaliza la anterior para un polinomio cualquiera $f(x)$ con coeficientes enteros.

5. $a = b + k.m \rightarrow a \equiv b(\text{mod } m)$.

6. $a = km \rightarrow a \equiv 0(\text{mod } m)$.

7. $a \equiv b(\text{mod } m) \wedge q|a \wedge q|b \wedge d = MCD(q,m) \rightarrow \frac{a}{q} \equiv \frac{b}{q}(\text{mod } \frac{m}{d})$. Esto es, si dos números enteros son congruentes módulo m y el entero q divide a ambos entonces los cocientes respectivos también son congruentes modulo m/d, siendo d el máximo común divisor de q y de m.

Demostración:

1. $a \equiv b(\text{mod } m) \leftrightarrow \begin{cases} a = mq_1 + r \\ b = mq_2 + r \end{cases} \leftrightarrow a - b = mq_1 - mq_2 = m(q_1 - q_2) \leftrightarrow a - b = km$

2. Puesto que $MCD(a,m) = 1 \leftrightarrow \exists x_1, x_2 \in Z / x_1 a + x_2 m = 1$, se tendría:

$$\begin{cases} x_1 a + x_2 m = 1 \\ a - b = km \end{cases} \rightarrow \begin{array}{l} x_1 a = 1 - x_2 m \\ x_1 a = x_1 km + x_1 b \end{array} \rightarrow 1 - x_2 m = x_1 km + x_1 b \rightarrow$$

$$\rightarrow x_1 b + (x_1 k + x_2)m = 1 \rightarrow \exists x_1, z_1 = x_1 k + x_2 \in Z / x_1 b + z_1 m = 1 \rightarrow MCD(b,m) = 1$$

3. Bastará probar que la diferencia es múltiplo de m:

$$(q_0 + a.q_1^n) - (q_0 + b.q_1^n) = q_1^n (a - b) \wedge a - b = km \rightarrow q_1^n (a - b) = km \rightarrow$$
$$\rightarrow (q_0 + a.q_1^n) \equiv (q_0 + b.q_1^n)(\text{mod } m)$$

4. Es una generalización trivial de la propiedad anterior.

5. Obviamente, pues $a - b = b + km - b = k.m \rightarrow a \equiv b(\text{mod } m)$

6. Trivial, pues $a - 0 = km - 0 = k.m \rightarrow a \equiv 0(\text{mod } m)$

7. Sea $q = q'.d$. Se tiene: $a \equiv b(\text{mod } m) \rightarrow a - b = km \rightarrow \frac{a}{q} - \frac{b}{q} = \frac{km}{q} = \frac{k}{q'}.\frac{m}{d}$, y como q divide a $k.m$, y d divide a m, q' tiene que dividir a k, luego la diferencia anterior se puede expresar como un múltiplo de m/d: $\frac{a}{q} - \frac{b}{q} = \frac{km}{q} = \frac{k}{q'}.\frac{m}{d} = K\frac{m}{d}$ lo que demuestra que $\frac{a}{q} \equiv \frac{b}{q}(\text{mod } \frac{m}{d})$

Ejemplo de aplicación de estas propiedades:

- En un caso como éste: $12 \equiv 7x(\mathrm{mod}\,5)$, se tiene que es equivalente escribir:

$$(2.5+2) \equiv 7x(\mathrm{mod}\,5) \rightarrow 2 \equiv 7x(\mathrm{mod}\,5) \rightarrow 2 \equiv (5x+2x)(\mathrm{mod}\,5) \rightarrow 2 \equiv 2x(\mathrm{mod}\,5) \rightarrow$$
$$\rightarrow 1 \equiv x(\mathrm{mod}\,5)$$

2.2. Congruencias lineales:

Son ecuaciones de la forma $a.x \equiv b(\mathrm{mod}\,m)$, donde m no divide a a.

Si x_1 es solución de la congruencia lineal, también es solución $x_1 + k_1 m$, cualquiera que sea el entero k_1. Los valores $x_1 + k_1 m$ representan la *clase residual* a la cual pertenece x_1:

$$a(x_1 + k_1 m) - b = km \rightarrow ax_1 - b = km \rightarrow ax_1 \equiv b(\mathrm{mod}\,m)$$

Así, si x_1 verifica la congruencia lineal, también la verifican todos los elementos de su clase residual: $x_1 + m, x_1 + 2m, \ldots$

Ejemplo:

La congruencia lineal $3.x \equiv 5(\mathrm{mod}\,2)$ es satisfecha, por ejemplo, por $x=1$. Y también la verifican los elementos de su clase residual: $1+2,\ 1+2.2,\ 1+3.2,\ \ldots 1+k_1.2,\ \ldots$

Sin embargo, usando la propiedad *5* de las congruencias, la congruencia lineal de este ejemplo es equivalente a $(2x+x) \equiv (4+1)(\mathrm{mod}\,2) \rightarrow x \equiv 1(\mathrm{mod}\,2)$

2.3. Soluciones congruentes y soluciones incongruentes:

Se denominan soluciones congruentes de una congruencia lineal módulo m a los enteros que las satisfacen y pertenecen a la misma clase residual módulo m.

Son soluciones incongruentes de una congruencia lineal módulo m a los enteros que la satisfacen y pertenecen a clases residuales distintas.

Por convenio, entenderemos que el conjunto solución de una congruencia lineal módulo m contiene exactamente un representante de cada una de las diferentes clases residuales módulo m cuyos miembros satisfacen la congruencia lineal dada. Esto es, las soluciones incongruentes que pertenecen a cualquier sistema completo de residuos módulo m constituye un conjunto solución.

El problema clave es, por consiguiente, determinar cuántas soluciones incongruentes, esto es, cuántas clases residuales, tiene la congruencia lineal dada. Veámoslo mediante un sencillo teorema.

Teorema 4:

La congruencia lineal $a.x \equiv b(\mathrm{mod}\,m)$ tiene exactamente d soluciones incongruentes, donde es $d = MCD(a,m)$ si y solo si d divide a b. Si d no divide a b, entonces la congruencia lineal no tiene solución.

Demostración:

Veamos en primer lugar que si es $d = MCD(a,m)$, entonces d ha de dividir a b.

$$ax \equiv b(\text{mod } m) \rightarrow ax - my = b \rightarrow \frac{a}{d}x - \frac{m}{d}y = \frac{b}{d} \rightarrow d \text{ ha de dividir a } b.$$

sean *a', b', M'* tales que *a=a'.d, b=b'.d, m=m'.d*.

Veamos ahora el número de soluciones incongruentes modulo m

$$ax \equiv b(\text{mod } m) \rightarrow ax - my = b \rightarrow \frac{a}{d}x - \frac{m}{d}y = \frac{b}{d} \rightarrow a'x - m'y = b' \text{ y } MCD(a',m')=1$$

solución de $a'x - m'y = b'$: $x = x_0 + m't$, $t=0,1,\ldots$, todas congruentes módulo m'.

Estas soluciones, que también son soluciones de la ecuación $ax - my = b$, aunque son congruentes modulo m' podrían, algunas de ellas, no ser congruentes modulo m. Vamos a encontrar las que no son congruentes modulo m.

Si dos de estas soluciones, $x_0 + m't_1$ y $x_0 + m't_2$, fueran congruentes módulo m, tendrían que verificar:

$$(x_0 + m't_1) \equiv (x_0 + m't_2)(\text{mod } m)$$

y, por las propiedades de las congruencias:

$$m't_1 \equiv m't_2(\text{mod } M)$$

o bien:

$$t_1 \equiv t_2(\text{mod } \frac{m}{m'}) \rightarrow t_1 \equiv t_2(\text{mod } d)$$

Es decir, los valores de t que dan soluciones $x = x_0 + m't$ congruentes modulo m son aquellos que son congruentes modulo d. Las soluciones $x = x_0 + m't$ incongruentes modulo m, son, por consiguiente, aquellas en las que figuren valores de t que no sean congruentes modulo d. Y, obviamente, como los valores de t son la sucesión $0,1,2,\ldots,n,\ldots$, los únicos que son incongruentes módulo d son aquellos menores que d: $0,1,2,\ldots,(d-1)$

Por tanto, las soluciones incongruentes de la congruencia lineal $a.x \equiv b(\text{mod } m)$ son la d soluciones $\{x_0, x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1).m'\}$, donde es d el Máximo Común Divisor de a y de m.

Ejemplo 1:

Hallemos las soluciones de la congruencia lineal $18x \equiv 24(\text{mod } 12)$.

Se tiene que $MCD(18,12) = 6$, que obviamente divide también a *24*, por lo que la congruencia tiene solución.

Dividiendo toda ella por 6 obtenemos la congruencia reducida: $3x \equiv 4(\mathrm{mod}\ 2)$, que se puede escribir como la ecuación diofántica: $3x - 2y = 4$, con solución particular $x_0=2$, $y_0=1$.

Los valores de x que verifican la ecuación son, en definitiva: $x = x_0 + m't,\ t = 0,1,\ldots$, esto es, $x = 2 + 2t,\ t = 0,1,\ldots$ que son soluciones congruentes modulo M', es decir, la ecuación reducida tiene una sola solución incongruente, que podemos representar, por ejemplo, por $x_0=2$.

Pero no todas estas soluciones congruentes modulo $m'=2$ son también congruentes modulo $m=12$. Así, no son congruentes modulo 12 aquellas que corresponden a valores de t que no sean congruentes modulo 6:

No son congruentes modulo 12 las soluciones en las que $t=0,1,2,3,4,5$, que serían:

$$2=2,\ 2+2.1=5,\ 2+2.2=6,\ 2+3.2=8,\ 2+4.2=10,\ 2+5.2=12$$

es decir, $2,4,6,8,10,12$

si restamos dos cualesquiera de ellas tendría que ser la diferencia un múltiplo de 12, lo cual no ocurre, y, sin embargo, verifica cada una de ellas la congruencia lineal $18x \equiv 24(\mathrm{mod}\ 12)$. Son por tanto soluciones incongruentes, cada una representando un conjunto infinito de soluciones entre si congruentes:

$$\{2\} = \{2,14,26,38,\ldots\},\ \{4\} = \{4,16,28,40,\ldots\},\ \{6\} = \{6,18,30,42,\ldots\},\ \{8\} = \{8,20,32,44,\ldots\}$$
$$\{10\} = \{10,22,34,46,\ldots\},\ \{12\} = \{12,24,36,48,\ldots\}$$

Ejemplo 2:

Hallemos las soluciones de la congruencia lineal $39x \equiv 60(\mathrm{mod}\ 6)$.

Se tiene que $MCD(39,6) = 3$, que obviamente divide también a 60, por lo que la congruencia tiene solución.

Dividiendo toda ella por 3 obtenemos la congruencia lineal reducida: $13x \equiv 20(\mathrm{mod}\ 2)$, que se puede escribir como la ecuación diofántica: $13x - 2y = 20$, con solución particular $x_0=2$, $y_0=3$.

Soluciones de la congruencia lineal reducida: $x = 2 + 2t, t = 0,1,2,\ldots$, y los valores de t que son incongruentes modulo 3: $t=0,\ t=1,\ t=2$. Por tanto, las soluciones incongruentes modulo 6, de la congruencia lineal de partida son: $2,4,6$, cada una de ellas, representando obviamente los infinitos elementos de una clase residual:

$$\{2\} = \{2,8,14,20,\ldots\},\ \{4\} = \{4,10,16,22,\ldots\},\ \{6\} = \{6,12,18,24,\ldots\}$$

4. Resolución de ecuaciones diofánticas lineales por aplicación de las congruencias lineales:

4.1. El caso de dos incógnitas:

Veamos a continuación un par de ejemplos resueltos usando congruencias lineales, y, también, usando el teorema 2, con el método de Euler para la solución particular.

a) Resolución de la ecuación diofántica $5x + 2y = 9$.

- Transformamos la ecuación en una congruencia lineal de módulo -2

$$5x + 2y = 9 \rightarrow 5x \equiv 9(\mathrm{mod}\,(-2)) \rightarrow x \equiv 1(\mathrm{mod}\,(-2)) \rightarrow x_0 = 1 \rightarrow x = 1 - 2t$$

Hallamos la otra incógnita sustituyendo en la ecuación:

$$5(1-2t) + 2y = 9 \rightarrow y = \frac{9 - 5 + 10t}{2} = 2 + 5t$$

Solución general: $(x, y) = (1 - 2t, 2 + 5t), \quad \forall t \in Z$, que verifica, como podemos comprobar, la ecuación diofantica de partida:

$$5x + 2y = 5(1-2t) + 2(2+5t) = 5 - 10t + 4 + 10t = 9$$

- Resolvamos de nuevo esta ecuación usando ahora el teorema 2 y el método de Euler:

Solución general, por el teorema 2:

$$\left.\begin{aligned} x &= x_0 - \frac{b}{d}t \\ y &= y_0 + \frac{a}{d}t \end{aligned}\right\} \rightarrow \left.\begin{aligned} x &= x_0 - 2t \\ y &= y_0 + 5t \end{aligned}\right\}$$

Usamos Euler: *5=2.2+1, 9=4.2+1*, con lo cual:

$$5x + 2y = 9 \rightarrow 2y = 2.4 + 1 - (2.2 + 1).x \rightarrow y = 4 - 2x + \frac{1 - x}{2}$$

Probamos valores de x:

$x = 0 \rightarrow \frac{1-0}{2} = \frac{1}{2} \notin Z$, no valido

$x = 1 \rightarrow \frac{1-1}{2} = 0 \in Z$, valido

$x_0 = 1, \; y_0 = \frac{9-5}{2} = 2$

y la solución general es $(x, y) = (1 - 2t, 2 + 5t), \quad \forall t \in Z$, que como ya hemos visto, verifica la ecuación diofántica de partida.

b) Resolución de la ecuación diofántica $3x - 7y = 5$.

- Mediante congruencias lineales:

$3x-7y=5 \rightarrow 3x \equiv 5(\mathrm{mod}\ 7) \rightarrow x_0 = 4$, por lo que $x = x_0 + \frac{m}{d}t = 4+7t$

y la segunda incógnita:

$$y = \frac{3x-5}{7} = \frac{3(4+7t)-5}{7} = \frac{7+21t}{7} = 1+3t$$

Solución general: $(x,y) = (4+7t, 1+3t), \quad \forall t \in Z$, que verifica, obviamente la ecuación diofántica de partida:

$$3(4+7t) - 7(1+3t) = 12 - 7 + 12t - 12t = 5$$

- Mediante el teorema 2 y Euler:

Solución general:

$$\left.\begin{array}{l} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{array}\right\} \rightarrow \left.\begin{array}{l} x = x_0 - 7t \\ y = y_0 - 3t \end{array}\right\}$$

Usamos Euler: *7=3.2+1, 5=2.2+1*, con lo cual:

$$3x-7y=5 \rightarrow 3x = 2.2.+1-(2.3+1).y \rightarrow x = 1+2y+\frac{2+y}{3}$$

Probamos valores de y:

$y = 0 \rightarrow \frac{2+0}{3} = \frac{2}{3} \notin Z,$ no valido

$y = 1 \rightarrow \frac{2+1}{3} = 1 \in Z,$ valido

$y_0 = 1, \ x_0 = 1+2+\frac{2+1}{2} = 4$

y la solución general es $(x,y) = (4-7t, 1-3t), \quad \forall t \in Z$ que también vemos que verifica la ecuación de partida: $3(4-7t) - 7(1-3t) = 12 - 7 - 12t + 12t = 5$

4.2. Ecuaciones diofánticas lineales con mayor número de incógnitas:

Veamos también aquí un par de ejemplos con 3 incógnitas resuelto mediante congruencias lineales:

a) Sea la ecuación diofántica lineal con tres incógnitas $3x-2y+5z=2$

$$3x-2y+5z=2 \rightarrow 3x+5z \equiv 2(\mathrm{mod}\ 2) \rightarrow x+z \equiv 2(\mathrm{mod}\ 2) \rightarrow x+z-2 = 2m$$

llamamos z=n y despejamos x: $x = 2+2m-n$

Finalmente, despejamos la incógnita *y* en la ecuación diofantica lineal de partida:

$2y = 3x + 5z - 2 = 3(2 + 2m - n) + 5n - 2 = 6 + 6m - 3n + 5n - 2 = 4 + 6m + 2n \rightarrow$
$\rightarrow y = 2 + 3m + n$

Solución general: $(x, y, z) = (2 + 2m - n, 2 + 3m + n, n), \quad \forall m, n \in Z$

Hacemos la comprobación:

$3(2 + 2m - n) - 2(2 + 3m + n) + 5n = 6 + 6m - 3n - 4 - 6m - 2n + 5n = 2$

b) Sea la ecuación diofántica lineal con tres incógnitas $7x + 3y + 2z = 17$
$7x + 3y + 2z = 17 \rightarrow 7x + 3y \equiv 17(\text{mod} - 2) \rightarrow x + y \equiv 1(\text{mod} - 2) \rightarrow$
$\rightarrow x + y - 1 = -2m$

llamamos $y=n$ y despejamos x: $x = 1 - 2m - n$

Finalmente, despejamos la incógnita z en la ecuación diofantica lineal de partida:

$$2z = 17 - 7x - 3y = 17 - 7(1 - 2m - n) - 3n = 17 - 7 + 14m - 7n - 3n =$$
$$= 10 + 14m + 4n \rightarrow z = 5 + 7m + 2n$$

Solución general: $(x, y, z) = (1 - 2m - n, n, 5 + 7m + 2n), \quad \forall m, n \in Z$

Hacemos la comprobación:

$7(1 - 2m - n) + 3n + 2(5 + 7m + 2n) = 7 - 14m - 7n + 3n + 10 + 14m + 4n = 17$

Bibliografía:

Burton W. Jones; *Teoría de los Números*, Editorial Trillas, México, 1969
Anthony J. Pettofrezzo; Donald R. Byrkit; *Introducción a la Teoría de los Números*, Limusa, 1972.
Williams Le Veque; *Teoría Elemental de los Números*, Herrero Hermanos, 1968
Goldfrey Harold Hardy; Edward Maitland Wright; *An Introduction to the Theory of Numbers*, Oxford University Press, 2008