Ecuaciones diofánticas lineales

Kenny J. Tinoco

Septiembre 2024

1. Definiciones

Antes de empezar recordemos lo siguiente.

Definición 1.1 (Máximo divisor común)**.** Dados $a, b \in \mathbb{Z}^{\neq 0}$, el máximo $d \in \mathbb{Z}^{+}$ tal que $d \mid a$ y $d \mid b$ es el máximo divisor común, y lo denotamos por $d = \text{mcd}(a, b)$.

Definición 1.2. Si $a, b \in \mathbb{Z}^{\neq 0}$ con $\text{mcd}(a, b) = 1$, entonces diremos que a y b son coprimos, primos relativos o primos entre sí.

Definición 1.3 (Combinación lineal)**.** Dados los enteros $a_1, a_2, \ldots, a_k$ definimos una combinación lineal de los a_i como un número de la forma

$$a_1x_1 + a_2x_2 + \ldots + a_kx_k$$

donde los x_i son enteros cualesquiera.

Teorema 1.1 (Algoritmo de la división)**.** Si $a, b \in \mathbb{Z}$ con $b \neq 0$, entonces existen enteros únicos (q, r) tales que $a = bq + r$ con $0 \leq r < |b|$.

Con el siguiente resultado es un teorema muy conocido e importante en la teoría de números y con el damos inicio al estudio de las ecuaciones diofánticas lineales, este resultado es utilizado tanto para la demostración de teoremas como la resolución de problemas.

Teorema 1.2 (Bezout)**.** Si $d = \text{mcd}(a, b)$, entonces d es el menor entero tal que

$$ax + by = d, \text{ para enteros } x, y.$$

Demostración. Sea S el conjunto de todos los enteros k tales que $ax + by = k$, debido a que la ecuación es sobre los números enteros podemos asegurar que S no es vacío, por lo tanto, debe existir un elemento mínimo k_1. Con esto, nuestro objetivo será demostrar que $k_1 = \text{mcd}(a, b)$. Sin embargo, como k_1 es una combinación lineal de a, b esto implica que k_1 es múltiplo de $\text{mcd}(a, b)$, con lo cual solo basta probar que $k_1 \mid a$ y $k_1 \mid b$, pero si esto es así, es equivalente a probar que k_1 divide a cualquier combinación

lineal de a, b, es decir, todo elemento de S. Procedamos por contradicción, sea $n \in S$ un elemento cualquiera y digamos que k_1 no divide a n, por el algoritmo de la división tenemos que $n = k_1 q + r$ para algunos enteros q, r con $0 < r < k_1$. Ahora bien, como n y k_1 son combinaciones lineales de a, b, entonces $r = n - k_1 q$ también es combinación lineal. Por lo tanto, r es un entero positivo menor a k_1 que pertenece a S, lo cual es una contradicción a la minimalidad de k_1. Luego, k_1 divide a todo $n \in S$ y por consiguiente $k_1 = \text{mcd}(a, b)$. ■

Teorema 1.3. La ecuación diofántica $ax + by = c$ tendrá soluciones si y solo si $\text{mcd}(a, b) \mid c$. Además, si (x_0, y_0) es una solución particular, entonces la solución general es

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

Demostración. Veamos la primera premisa, si $d = \text{mcd}(a, b)$, entonces $a = a_1 d$ y $b = b_1 d$, sustituyendo en la ecuación original obtenemos que $d(a_1 x + b_1 y) = c$ por lo cual d divide a c. Ahora, por el teorema de bezout existen x_1, y_1 tales que

$$ax_1 + by_1 = d.$$

Ya que $c = kd$, al multiplicar el resultado anterior por k, obtenemos

$$akx_1 + bky_1 = kd \iff a(kx_1) + b(ky_1) = c,$$

donde las soluciones son $(x, y) = (kx_1, ky_1)$. Veamos la segunda premisa, sea (x_0, y_0) una solución de la ecuación, al sustituir en la ecuación original, vemos que

$$\begin{aligned} ax + by = c = ax_0 + by_0 \\ \iff a(x - x_0) = b(y_0 - y) \\ \iff a_1 d(x - x_0) = b_1 d(y_0 - y) \\ \iff a_1(x - x_0) = b_1(y_0 - y) \end{aligned}$$

Como a_1 y b_1 son coprimos, tenemos que $b_1 \mid (x - x_0)$ por lo cual $(x - x_0) = b_1 t$ donde t es entero, sustituyendo en el resultado anterior, obtenemos $(y_0 - y) = a_1 t$, luego las soluciones son

$$(x, y) = (x_0 + b_1 t, y_0 - a_1 t), \quad \text{con } a_1 = \frac{a}{d},\ b_1 = \frac{b}{d}.$$ ■

Ahora veamos algunos ejemplos.

Ejemplo 1.1. Resolver la ecuación $5x - 3y = 52$ en enteros positivos.

Solución. Primero, como $\text{mcd}(5, 3) = 1$ y $1 \mid 52$, entonces la ecuación tiene soluciones enteras. Ahora, analizando en módulo 5 tenemos que

$$-3y \equiv 52 \ (\text{mód } 5) \implies 2y \equiv 2 \ (\text{mód } 5) \implies y \equiv 1 \ (\text{mód } 5).$$

Claramente $y = 1$ es solución a esta congruencia, sustituyendo en la ecuación original $5x - 3 \cdot 1 = 52 \iff 5x = 55$ por lo cual, la ecuación tiene una solución $(11, 1)$, luego con la solución $(x_0, y_0) = (11, 1)$ llegamos a

$$(x, y) = (11 + 3t, 1 - 5t), \text{ donde } t \in \mathbb{Z}. \qquad \blacksquare$$

Ejemplo 1.2. Resolver la siguiente ecuación $8c + 7p = 100$.

Solución. Claramente la ecuación tiene soluciones enteras, analizando en módulo 8,

$$7p \equiv 100 \text{ (mód 8)} \implies -p \equiv 4 \text{ (mód 8)} \implies p \equiv -4 \text{ (mód 8)} \implies p \equiv 4 \text{ (mód 8)}.$$

Rápidamente, podemos decir que $p = 4$ es una solución para dicha congruencia, sustituyendo en la ecuación obtenemos $c = 9$. Luego, con la solución $(c_0, p_0) = (9, 4)$ tenemos

$$(c, p) = (9 + 7t, 4 - 8t), \quad \text{con } t \in \mathbb{Z}. \qquad \blacksquare$$

2. Aplicando el algoritmo de Euclides

Definición 2.1 (Algoritmo de Euclides)**.** Si $a, b \in \mathbb{Z}^{\neq 0}$ y $a = bq + r$ para algunos enteros q, r con $0 < r < b$, entonces

$$\text{mcd}(a, b) = \text{mcd}(b, r).$$

Podemos usar este algoritmo para resolver ecuaciones lineales de una manera iterativa, similar, a la manera en cómo se calcula el MCD de dos números grandes.

Sean $a, b, c \in \mathbb{Z}$ con $a, b \neq 0$ y $d = \text{mcd}(a, b)$, considerando la ecuación

$$ax + by = c,$$

se tienen los siguientes pasos:

1. Si $d \nmid c$, entonces no hay solución.
2. Si $d \mid c$, entonces se divide la ecuación por d obteniendo $a_1 x + b_1 y = c_1$.
3. Por el paso anterior la ecuación tiene coeficiente coprimos;
   - 3.1. Si $a_1 \mid c_1$, entonces $a_1 c_0 = c_1$, luego $(x, y) = (c_0, 0)$ es solución.
   - 3.2. Si $a_1 \nmid c_1$, entonces tomamos el menor de $|a_1|, |b_1|$ y obtenemos[1]

   $$b_1 = a_1 q_1 + r_1, \text{ con } 0 < r_1 < |a|, \qquad c_1 = a_1 q_2 + r_2, \text{ con } 0 < r_2 < |a|.$$

4. Sustituimos en la ecuación

   $$a_1 x + (a_1 q_1 + r_1) y = a_1 q_2 + r_2 \iff a_1(x + q_1 y - q_2) + r_1 y = r_2.$$

   Haciendo $z = x + q_1 y - q_2$, la ecuación anterior se transforma en $a_1 z + r_1 y = r_2$.

[1] Aquí vamos suponer que $|a_1|$ es el menor.

4.1. Si $r_1 \mid r_2$, entonces terminamos con el paso 3.1.

4.2. Si $r_1 \nmid r_2$, entonces vamos al paso 3.2 y repetimos el proceso.

Con estos pasos (o algoritmo) es posible resolver ecuaciones diofánticas lineales con coeficientes grandes, de una manera cíclica o iterativa, lo cual reduce la complejidad de resolver la ecuación diofántica, esto lo podemos apreciar en la figura 1.

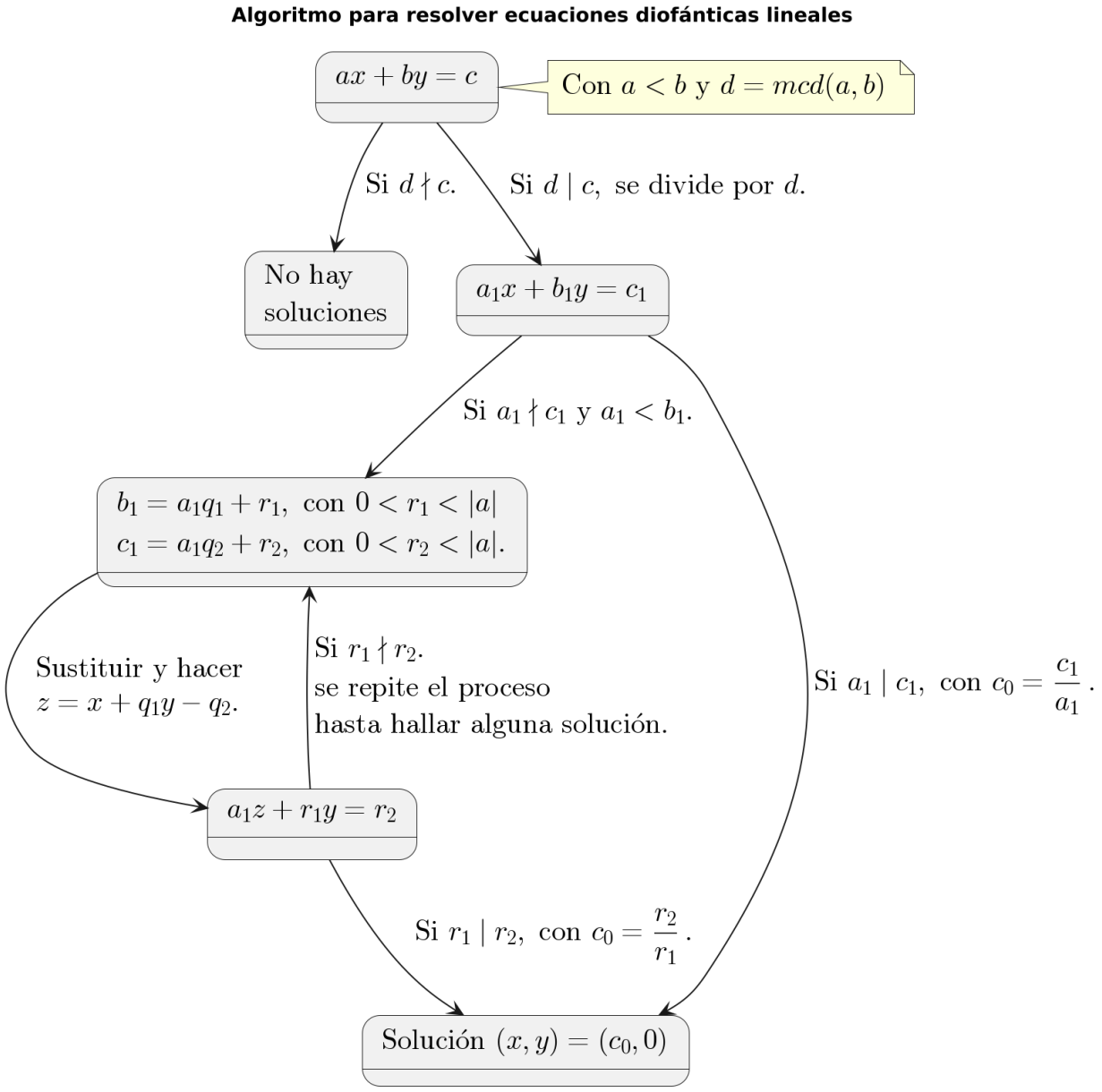

Figura 1: Diagrama de estado para resolver ecuaciones diofánticas lineales.

Veamos algunos ejemplos.

Ejemplo 2.1. Resuelva la siguiente ecuación $350x + 425y = 1200$.

Solución. Como $\text{mcd}(350, 425) = 25$ y $25 \mid 1200$, dividimos ambos lados de la ecuación por 25 y tenemos

$$14x + 17y = 48$$

Por el algoritmo de euclides se tiene que $17 = 1 \cdot 14 + 3$ y $48 = 3 \cdot 14 + 6$. Sustituyendo y agrupando, tenemos $14(x + y - 3) + 3y = 6$. Haciendo $z = x + y - 3$ y sustituyendo en esta última ecuación se tiene $14z + 3y = 6$. Como $3 \mid 6$, para esta ecuación tenemos una solución de la forma $z = 0$ y $y = 2$. Escribiendo z en términos de x y $y = 2$, obtenemos el valor de $x = 1$. Luego, la solución general de la ecuación inicial es:

$$x = 1 + 17k, \quad y = 2 - 14k, \quad \text{con } k \in \mathbb{Z}. \qquad \blacksquare$$

3. Caso general de ecuaciones lineales

Hasta el momento sólo hemos trabajado en ecuaciones lineales de dos variables, pero en realidad la ecuación $ax + by = c$ no es más que un caso particular de la ecuación

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

donde $a_1, a_2, \ldots, a_n$, y c son coeficientes. También, cabe mencionar que el teorema de bezout también se cumple para una cantidad n de números, con lo cual se podrá hacer un tratamiento similar al caso concreto de $n = 2$.

Teorema 3.1. La ecuación diofántica $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ tiene solución si y solo si $\text{mcd}(a_1, a_2, \cdots, a_n) \mid c$.

Veamos un ejemplo.

Ejemplo 3.1. Resuelva la ecuación $3x + 4y + 5z = 6$.

Solución. Primero, notamos que $\text{mcd}(3, 4, 5) = 1$ efectivamente divide a 6. Trabajando en módulo 5 tenemos que $3x + 4y \equiv 1 \pmod 5$ por lo cual $3x + 4y = 1 + 5s$, con $s \in \mathbb{Z}$. Si tomamos a s como una constante, una solución para esta ecuación es $(x_0, y_0) = (-1 + 3s, 1 - s)$. Usando el teorema 1.3, obtenemos las soluciones generales de esta ecuación de dos variables

$$(x, y) = (-1 + 3s + 4t, 1 - s - 3t) \quad \text{con } t \in \mathbb{Z}.$$

Sustituyendo esto en la ecuación original obtenemos $z = 1 - s$, por lo que todas las soluciones son

$$(x, y, z) = (-1 + 3s + 4t, 1 - s - 3t, 1 - s), \quad \text{con } s, t \in \mathbb{Z}. \qquad \blacksquare$$

Como vemos en este ejemplo, una ecuación de tres variables la podemos reducir a una ecuación de dos variables, ecuación que sabemos cómo solucionarla, luego solo debemos revertir el proceso y dejar las soluciones en función de los parámetros que aparezcan. Análogamente, podemos resolver una ecuación de grado n reduciéndola sucesivamente a una de grado dos y realizar un proceso similar.

4. Existencia de soluciones

Para concluir, veremos algunos resultados que estudian la existencia de soluciones para una ecuación diofántica, estos resultados ya son parte de una teoría de mayor complejidad, si se tiene curiosidad se invita al lector a investigar más a fondo.

Definición 4.1. Sean $a_1, a_2, \ldots, a_n$ enteros positivos con $\text{mcd}(a_1, a_2, \ldots, a_n) = 1$ se define a $g(a_1, a_2, \ldots, a_n)$ como el mayor entero positivo N para el cual

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = N,$$

no tiene soluciones enteras.

El problema de determinar $g(a_1, \ldots, a_n)$ es conocido como el problema de las monedas de Frobenius. Este problema fue planteado por Ferdinand Frobenius, quien se interesó en encontrar la mayor cantidad de dinero que no se puede representar como una combinación lineal de n denominaciones de monedas, quizás el ejemplo más sencillo es con monedas de 3 y 5 centavos con las cuales nunca se podrá pagar una deuda de 7 centavos. El siguiente teorema brinda un valor de N para el caso de $n = 2$.

Teorema 4.1 (Sylvester)**.** Sean $a, b \in \mathbb{Z}^+$, con $\text{mcd}(a, b) = 1$, entonces

$$g(a, b) = ab - a - b.$$

Con esto se puede analizar la ecuación $3x + 5y = 7$, como $g(3, 5) = 3 \cdot 5 - 3 - 5 = 7$ entonces se tiene que 7 es el mayor entero para el cual no hay soluciones. Para los casos de $n \geq 2$ hasta la fecha no se conoce ninguna fórmula explícita de g, cabe aclarar que estos temas ya son de una complejidad mayor a este curso. Finalmente, con el teorema sylvester podemos entender mejor el siguiente resultado.

Teorema 4.2 (Chicken McNugget)**.** Sean[a] $a, b \in \mathbb{Z}^+$ con $\text{mcd}(a, b) = 1$, se tiene:

i. Si $n = ab - a - b$, entonces $ax + by = n$ es insoluble $\forall x, y \in \mathbb{Z}^+$.

ii. Si $n > ab - a - b$, entonces la ecuación es soluble.

[a] Su historia es curiosa, debido a que fue enunciado en un McDonald's.

Como recomendación general, se aconseja siempre verificar que una ecuación cumpla con el segundo punto del teorema anterior.

5. Ejercicios y problemas

Ejercicios y problemas para el autoestudio.

Ejercicio 1. ¿Tiene la ecuación $24x + 18y = 12$ soluciones enteras?

Ejercicio 2. Resuelva la ecuación diofántica $125x - 25y = 28$.

Ejercicio 3. Resuelva la ecuación $69x + 123y = 3000$.