# Ecuaciones Diofánticas Lineales

Pablo L. De Nápoli

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Álgebra I - Primer cuatrimestre de 2020

# Ecuaciones Diofánticas

Una ecuación diofántica es una ecuación en la que interesa encontrar las soluciones enteras (reciben este nombre en honor al matemático Diofanto de Alejandría (siglo III) que las estudió.

Una ecuación diofántica lineal en dos variables es una ecuación de la forma:

$$a \cdot x + b \cdot y = c$$

siendo $a$, $b$ y $c$ números enteros dados.

Geométricamente, este problema significa que buscamos los puntos en el plano de coordenadas enteras que estén situados sobre una recta.

# Criterio para Existencia de soluciones

**Teorema (Proposición 5.1.2 del apunte de la profesora Krick)**

*Llamemos $d = (a : b)$ al máximo común divisor entre los coeficientes $a$ y $b$. Entonces la ecuación diofántica $a \cdot x + b \cdot y = c$ admite soluciones si y sólo si $d|c$.*

La prueba es sencilla: si hay una solución $(x, y)$ entonces

$$d|a \wedge d|b \Rightarrow d|ax \wedge d|by \Rightarrow d|c.$$

Recíprocamente si $d|c$, consideramos $c' = c : d$. Entonces usando el algoritmo de Euclides extendido pordemos encontrar $s$ y $t$ tales que

$$s \cdot a + t \cdot b = d$$

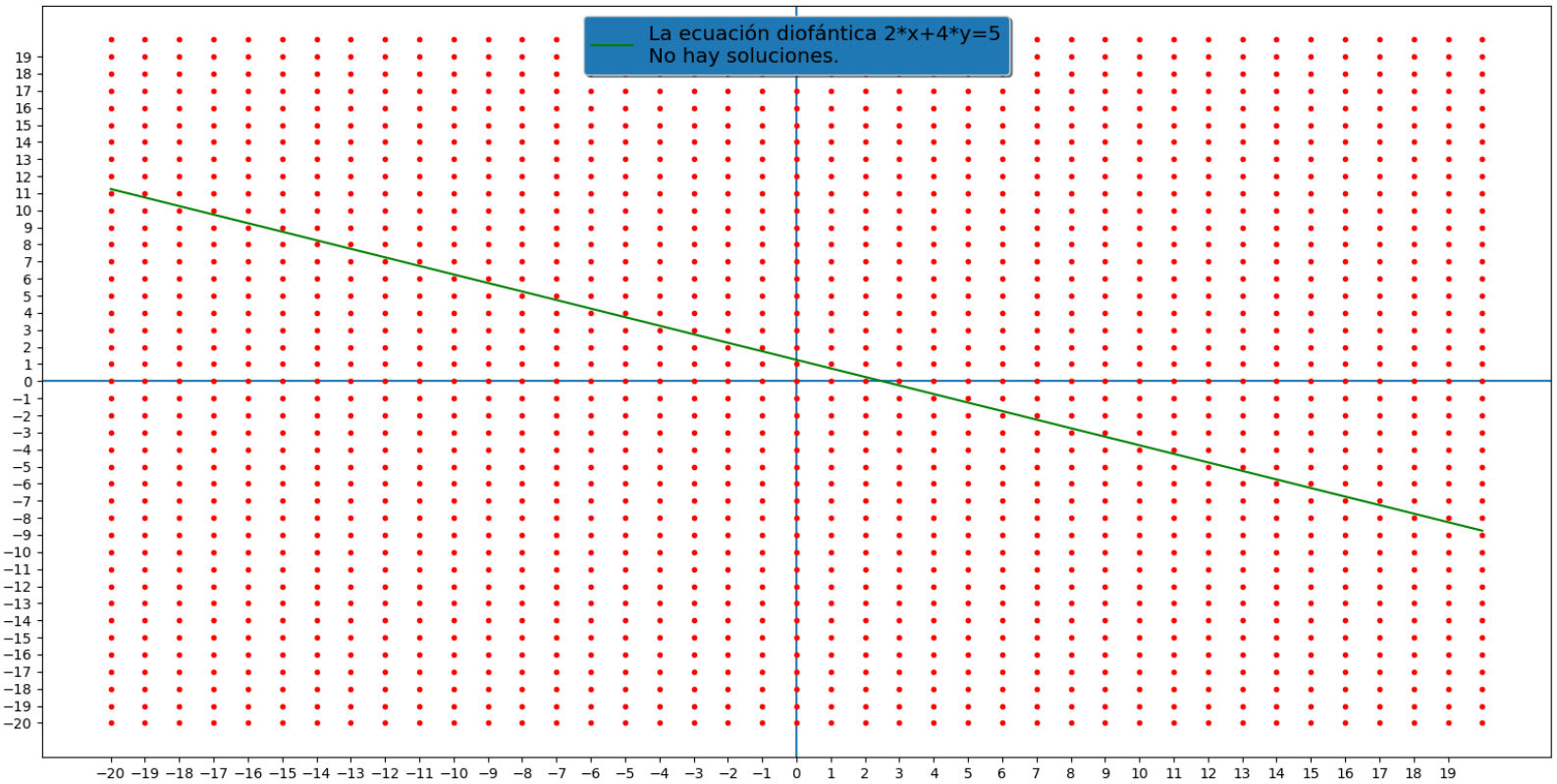
y multiplicando por $c'$ obtenemos:

$$(s \cdot c') \cdot a + (t \cdot c') \cdot b = c$$

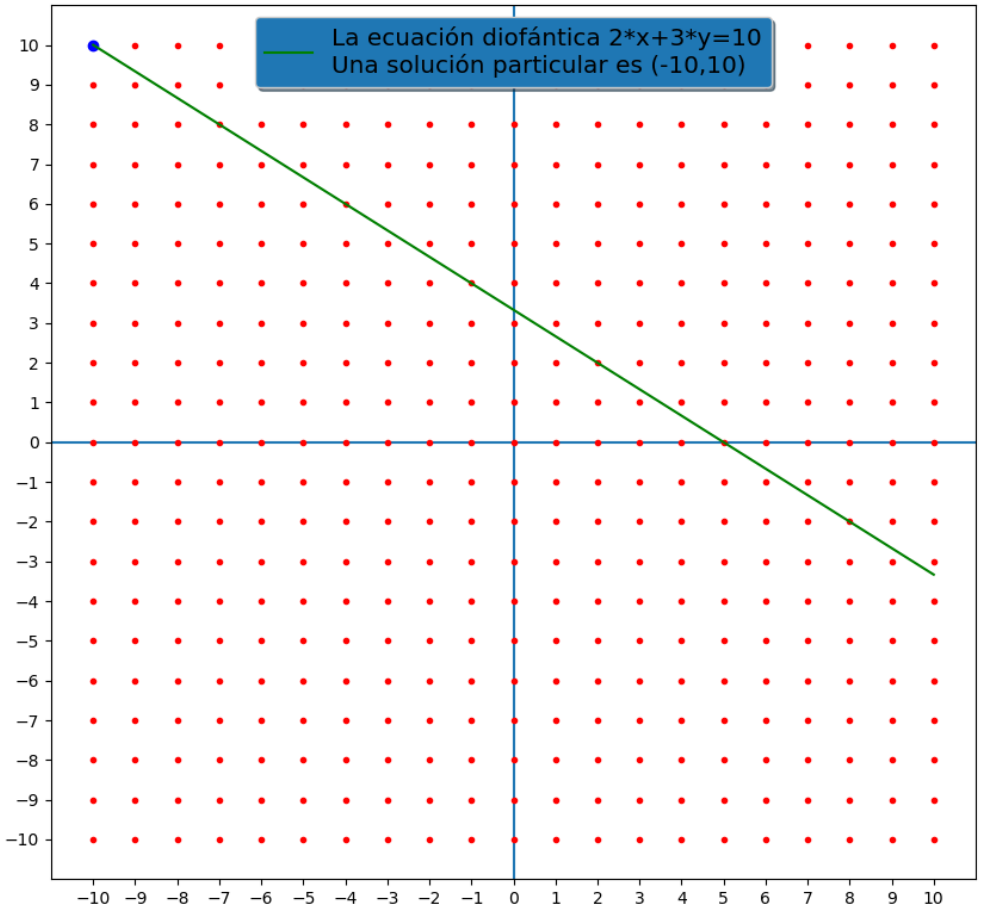
Por lo que $(x_0, y_0) = (s \cdot c', t \cdot c')$ es una solución particular de nuestra ecuación.

# Un ejemplo sin soluciones

La ecuación diofántica $2x + 4y = 5$ no tiene soluciones pues en este ejemplo $d = 2$ y $d$ no divide a 5. Esto es evidente en este ejemplo pues si hubiera una solución, el primer miembro sería par mientras que 5 es impar.



# Un ejemplo con soluciones




Aquí $d = 1$ y $s = -1$, $t = 1$.

# Dos observaciones clave

- Si estamos en el caso en que $d|c$, llamando $a' = a : d$, $b' = b : d$ (coprimalizando) obtenemos una ecuación equivalente

$$a' \cdot x + b' \cdot y = c'$$

Notemos que ahora $a'$ y $b'$ serán coprimos pues $s \cdot a' + t \cdot b' = 1$.

- Si $(x, y)$ es una solución cualquiera de nuestra ecuación y $(x_0, y_0)$ es la solución particularque encontramos antes

$$a' \cdot (x - x_0) + b' \cdot (y - y_0) = 0$$

así pues la diferencia $(x, y) - (x_0, y_0)$ satisfará la ecuación homogénea (con $c = c' = 0$). Luego: todas las soluciones se obtienen como la suma de una solución particular y una solución de la ecuación homogénea.

# Soluciones de la ecuación homogénea

Si tenemos una solución de la ecuación homogénea

$$a' \cdot x + b' \cdot y = 0$$

Podemos escribirla como

$$a' \cdot x = -b' \cdot y$$

Notamos que entonces $b' | a' \cdot x$, pero como $a' \perp b' \Rightarrow b' | x \Rightarrow x = k \cdot b'$. Similarmente $a' | b' \cdot y$, y como $a' \perp b' \Rightarrow a' | y \Rightarrow y = j \cdot a'$. Pero para que se cumpla la ecuación

$$a' \cdot (k \cdot b') + b' \cdot (j \cdot a') = 0$$

debe ser $j = -k$, luego todas las soluciones de la ecuación homogénea son de la forma:

$$(k \cdot b', -k \cdot a')$$

con $k$ entero.

# Todas las soluciones

Juntando estas observaciones, podemos completar el enunciado del teorema de la siguiente manera:

## Teorema (Proposición 5.1.6 del apunte)

*Cuando $d = (a : b) | c$ la ecuación diofántica $a \cdot x + b \cdot y = c$ admite infinitas soluciones. Todas ellas se pueden parametrizarse como*

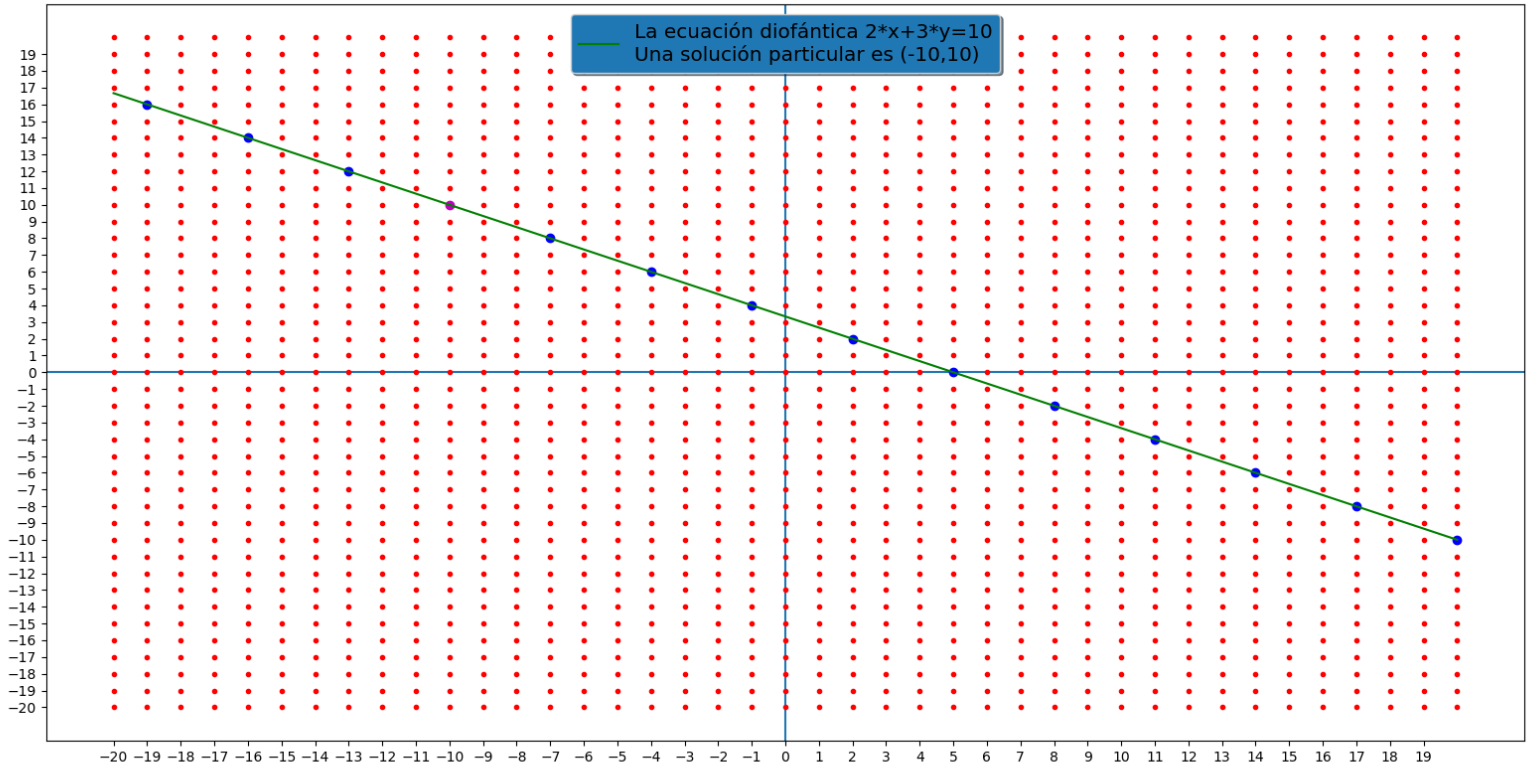
$$\begin{cases} x &= s \cdot c' + k \cdot b' \\ y &= t \cdot c' - k \cdot a' \end{cases} \qquad k \in \mathbb{Z}$$

*donde $a' = a : d, b' = b : d, c' = c : d$ y*

$$s \cdot a + t \cdot b = d$$

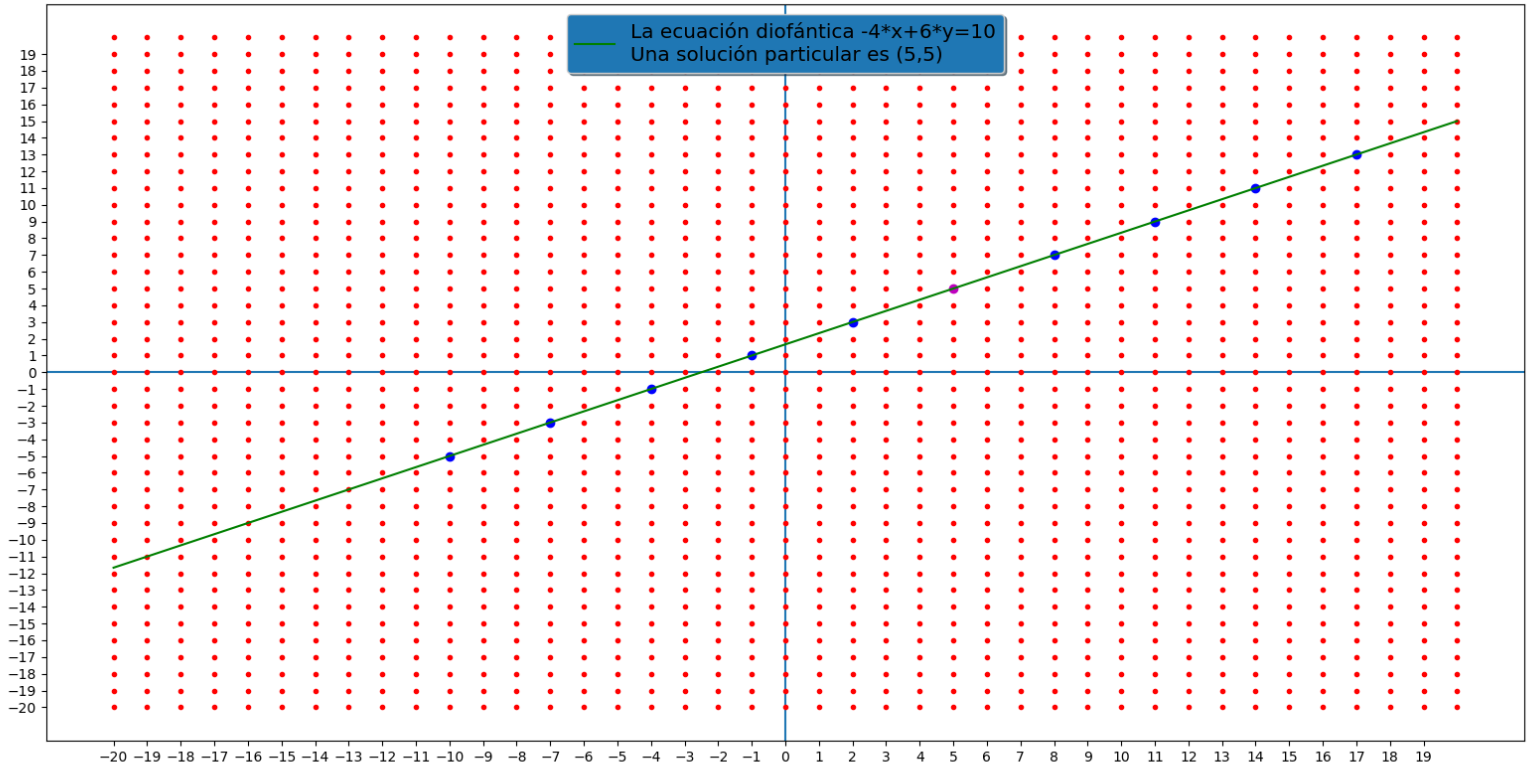
*($s$ y $t$ se encuentran usando el algoritmo de Euclides extendido)*

# Continuamos el ejemplo de antes..




Aquí $a = a' = 2$, $b = b' = 3$, $c = c' = 10$, $d = 1$, $s = -1$ y $t = 1$. Las soluciones son $(-10 + 3k, 10 + 2k)$ con $k \in \mathbb{Z}$.

# Otro ejemplo (con $d = 2$)




Aquí $a - 4, b = 6, c = 10, d = 2, a' = -2, b' = 3, c' = 5, s = -1, t = 1$.
Las soluciones son $(5 + 3k, 5 + 2k)$ con $k \in \mathbb{Z}$.

# Algunas cosas para pensar

¿Qué pasa con una ecución diofántica en tres variables?

$$a \cdot x + b \cdot y + c \cdot z = d$$

La noción de máximo común divisor se puede extender a más de dós números, y es una operación asociativa

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

Se deduce que el máximo común divisor de 3 números se puede escribir como una combinación lineal de ellos:

$$\text{mcd}(a, b, c) = s \cdot a + t \cdot b + r \cdot c$$

con $s, t, r$ enteros.
La teoría anterior se puede entonces extender a este caso. La ecuación tendrá solución si y sólo si $\text{mcd}(a, b, c) | d$.