3. ***Linear Diophantine equations.*** Let a, b, and c be natural numbers. Show that the linear equation

$$ax + by = c$$

has integer solutions x and y if and only if $gcd(a, b)$ divides c, and that it has either zero or infinitely many integer solutions. Then give a polynomial time algorithm that returns a solution (x, y) where the integers $x, y \geq 0$ or reports that no such solution exists.

Tenint qualsevol equació de la forma $a \cdot x + b \cdot y = c$, definim $g = gcd(a, b)$ com al màxim comú divisor entre a i b. Anem a provar les dues direccions de la implicació:

$a \cdot x + b \cdot y = c$ té solució (x, y) entera $\implies$ g divideix c:

Com que g divideix a i b, definim $a' = \frac{a}{g}$ i $b' = \frac{b}{g}$, si obtenim una nova expressió equivalent:

$$g \cdot a' \cdot x + g \cdot b' \cdot y = c \tag{1}$$

Podem factoritzar g, obtenint:

$$g \cdot (a' \cdot x + b' \cdot y) = c \tag{2}$$

Com que els dos factors de la part esquerra són enters, g és un divisor de c.

$a \cdot x + b \cdot y = c$ té solució (x, y) entera $\impliedby$ g divideix c:
Sabem que $gcd(a, b) = g$, i que podem usar l'algorisme d'Euclides ampliat per a trobar la seva identitat de Bézout (x', y') tal que

$$a \cdot x' + b \cdot y' = g \tag{3}$$

Donada aquesta equació, multipliquem els dos costats per $\frac{c}{g}$ obtenint:

$$\frac{c}{g} \cdot a \cdot x' + \frac{c}{g} \cdot b \cdot y' = c \tag{4}$$

Podem canviar l'ordre dels productes per a arribar a la solució final:

$$a \cdot (\frac{c \cdot x'}{g}) + b \cdot (\frac{c \cdot y'}{g}) = c \tag{5}$$

de manera que $(\frac{c \cdot x'}{g}, \frac{c \cdot y'}{g})$ és una solució.

Per a trobar dita solució algorísmicament tan sols cal trobar $g = gcd(a, b)$ i la identitat de Bézout de a i b (x', y'). Els dos es poden trobar en temps $O(log(min(a, b)))$ usant l'algorisme d'Euclides ampliat. Sabent aquestes dades, si g divideix c $(\frac{c \cdot x'}{g}, \frac{c \cdot y'}{g})$ s'ha demostrat abans que és una solució, si no el divideix s'ha demostrat que no en té i l'algorisme no retorna res.