Ejercicio 6. Sean $a, b \in \mathbb{Z}$ números enteros tales que $\text{mcd}(a, b) = 1$. Calcula $\text{mcd}(a + b, a - b)$ en función de a y b.

Solución 6.

Supongamos $\text{mcd}(a + b, a - b) = d$, esto implica $d|a + b$ y $d|a - b$. Así, existen $m, n \in \mathbb{Z}$ tales que $a + b = md$ y a - b = nd.

Sumando y restando ambas expresiones obtenemos : $2a = (m + n)d$ y $2b = (m - n)d$. De esta manera, tenemos también que $d|2a$ y $d|2b$. Ahora, aplicando el lema $\text{mcd}(ka, kb) = k * \text{mcd}(a, b)^*$, tenemos que $\text{mcd}(2a, 2b) = 2 * \text{mcd}(a, b) = 2 * 1 = 2$.

Así pues, sustituyendo las expresiones 2a y 2b por sus respectivos valores, obtenemos $\text{mcd}((m + n)d, (m - n)d) = d * \text{mcd}(m + n, m - n) = 2$. De esta igualdad obtenemos que d divide a dos, es decir, $d|2$. Por tanto, $d \leqslant 2$. Y como siempre tenemos en cuenta a mcd positivos, deducimos que d = 1 o d = 2.

* Demostración del lema: Dados a, b, k $\in \mathbb{Z}$, veamos que $\text{mcd}(ka, kb) = k * \text{mcd}(a, b)$.

Sea $d = \text{mcd}(a, b)$, entonces $d|a$ y $d|b$. Veamos que kd divide a ka y kb. Por $d|a$ y $d|b$ tenemos que existen e, f $\in \mathbb{Z}$ tales que a = de y b = df. Multiplicando ambos lados de cada ecuación por k obtenemos ka = k(de) = (kd)e y kb = k(df) = (kd)f. Queda probada así que $kd|ka$ y $kd|kb$.

Asumamos ahora que $g = \text{mcd}(ka, kb)$. Entonces $g|ka$ y $g|kb$. Teniendo en cuenta que g es el mcd, entonces cualquier otro divisor común de ka y kb ,si existe, es menor o igual que g. Aplicando esto a kd, tenemos que $kd \leqslant g$, y además $k|\text{mcd}(ka, kb)$. Luego $\exists l \in \mathbb{Z}$ tal que g = kl. Como $kd \leqslant g = kl$, exigimos $d \leqslant l$. Pero además, $l|a$ y $l|b$, dado que $g|ka$ y $g|kb$. Sin embargo, por otra parte, $l \leqslant d$, ya que d es el mcd de a y b.

Como $d \leqslant l$ y $l \leqslant d$, llegamos a que d = l. Por tanto, g = kl = kd = k * $\text{mcd}(a, b)$, y queda demostrada el lema.