

Recuerda que teníamos:

Teorema III. Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Si d es la mínima combinación lineal positiva de a y b , entonces $d = \text{mcd}(a, b)$.

Aparentemente este teorema es una "implicación", así que me preguntaron si se puede usar como un "si y solo si".

En otras palabras, me preguntaron si el Teorema III se puede escribir de la siguiente manera:

Teorema III modificado.

Sean $a, b, d \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Entonces d es la mínima com

combinación lineal positiva de a y $b \iff d = \text{mcd}(a, b)$.

La respuesta es que SI y el argumento es sencillo:

\Rightarrow) esta implicación es tal cual el **Teorema III**

\Leftarrow) Suponemos que $d = \text{mcd}(a, b)$.

Tomemos la mínima combinación lineal positiva de a y b , y llamemos w a tal combinación lineal.

Lo que hay que argumentar es que $w = d$. Pero

el **Teorema III** dice que

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

Por lo tanto, $w = d$.

□

Como puedes ver, el "regreso" del **Teorema III modificado** se

Prueba con el mismo Teorema III, así que en realidad puedes pensarlos como teoremas equivalentes.