Teorema. Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Si $c \in \mathbb{Z} \setminus \{0\}$, entonces

$$mcd(ac, bc) = |c| \, mcd(a, b).$$

Prueba.

Haremos la prueba en dos pasos:

Paso 1. Probaremos que

$$mcd(ac, bc) \leq |c| \, mcd(a, b).$$

Paso 2. Probaremos que

$$mcd(ac, bc) \geq |c| \, mcd(a, b).$$

Una vez concluidos los dos pasos, obtendremos la igualdad que queremos.

Prueba del Paso 1.

Queremos probar que

$$\boxed{mcd(ac, bc) \leq |c| \, mcd(a, b)}$$

Para esto, recuerda lo que

decía el Teorema III.

Entre otras cosas, ese teorema decía que mcd(a,b) es combinación lineal de a y b. i.e. $\exists \alpha, \beta \in \mathbb{Z}$ tales que

$$\text{mcd}(a,b) = \alpha a + \beta b$$

Así que

$$(\star_1) \quad |c|\,\text{mcd}(a,b) = |c|(\alpha a + \beta b)$$
$$= |c|\alpha a + |c|\beta b.$$

¿Sabemos algo de $|c|$?

Por hipótesis tenemos que $c \neq 0$, pero no sabemos si $c > 0$ o si $c < 0$, así que tomaremos dos casos:

<u>Caso 1</u>. Si $c > 0$.

Por $(\star_1)$, en este caso se tiene

$$|c|\,\text{mcd}(a,b) = (\alpha)ac + (\beta)bc$$

En otras palabras,

$|c|\,\text{mcd}(a,b)$ es combinación

lineal de ac y bc
(esto es importante, recuérdalo)

Caso 2. Si $c<0$

Usando ($\star_1$) de nuevo, en este caso obtenemos

$$|c|\, mcd(a,b) = (-c)\alpha a + (-c)\beta b$$
$$= (-\alpha) ac + (-\beta) bc$$

Así, en este caso $|c|\, mcd(a,b)$ es combinación lineal de ac y bc.

Como puedes ver, en ambos casos obtuvimos que $|c|\, mcd(a,b)$ es combinación lineal de ac y bc.

Ahora, ¿es $|c|\, mcd(a,b) > 0$?

Bueno, $|c| > 0$ y $mcd(a,b) \geq 1$, así que, en efecto, el número $|c|\, mcd(a,b)$ es positivo.

Esto quiere decir que

$|c|\, mcd(a,b)$ es una combinación

lineal positiva de ac y bc.

¿Te suena a algo?

¿Quién es la mínima combinación lineal positiva de ac y bc?

¡Claro! es mcd (ac, bc)

(por el Teorema III)

Esto quiere decir que

mcd (ac, bc) es menor o igual que cualquier combinación lineal positiva de ac y bc.

$$\boxed{\therefore \ \text{mcd}(ac, bc) \leq |c| \, \text{mcd}(a, b).}$$

Ya terminamos el Paso 1 ☺

Prueba del Paso 2.

Ahora probaremos que

$$\text{mcd}(ac, bc) \geq |c| \, \text{mcd}(a, b)$$

Por el primer inciso de la

Definición II sabemos que

$$\text{mcd}(a,b) \mid a \quad y$$

$$\text{mcd}(a,b) \mid b$$

Por otro lado, ya hemos visto que $|c| \mid c$.

Usando todo esto y el Lema (César) obtenemos que

$$|c| \, \text{mcd}(a,b) \mid ca \quad y$$

$$|c| \, \text{mcd}(a,b) \mid cb$$

Es decir, el número $|c| \, \text{mcd}(a,b)$ es un divisor común de ca y cb.

Así, por la Definición II (parte ii), concluimos que

$$\boxed{|c| \, \text{mcd}(a,b) \leq \text{mcd}(ac, bc).}$$

Ya terminamos el Paso 2 ☺

$\therefore |c| \operatorname{mcd}(a,b) = \operatorname{mcd}(ac, bc)$.

$\square$

Última modificación: 8:42 p. m.