En clase mencionamos que daríamos 4 formas de ver al máximo común divisor. Tenemos:

La Definición I

La Definición II

El Teorema III

Ahora daremos la cuarta forma de ver al máximo común divisor:

Definición IV: Sean $a, b, d \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Decimos que $d = \text{mcd}(a,b)$ si se cumplen:

1) $d \geq 1$
2) $d \mid a$ y $d \mid b$
3) $\forall d' \in \mathbb{Z}$

$$d' \mid a \text{ y } d' \mid b \Rightarrow d' \mid d.$$

Como puedes ver, la Definición IV se parece mucho a la Definición II.

¿Cómo iba la Definición II?

<u>Definición II</u>. Sean $a, b, d \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Decimos que $d = \text{mcd}(a,b)$ si:

i) $d \mid a$ y $d \mid b$

ii) $\forall d' \in \mathbb{Z}$ se tiene

$$d' \mid a \text{ y } d' \mid b \Rightarrow d' \leq d.$$

Aunque se parecen mucho, la Definición II y la Definición IV no son iguales. Si realmente ambas definen al máximo común divisor, sería necesario probarlo. Vamos a hacerlo a continuación.

<u>Teorema</u>. Sean $a, b, d \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Entonces d cumple la Definición II $\iff$ d cumple la Definición IV.

Prueba.

$\Rightarrow$) Supongamos que d cumple la Definición II.

$\boxed{\text{P.D. } d \text{ cumple la Definición IV}}$

Observa que $1|a$ y $1|b$.

Por ii) de la Definición II obtenemos que $1 \leq d$.

Esto prueba i) de la Definición IV.

El siguiente paso es fácil: como d cumple i) de la Definición II, entonces cumple 2) de la Definición IV.

Falta probar que d cumple 3) de la Definición IV.

Para esto, sea $d' \in \mathbb{Z}$ y supongamos que $d'|a$ y $d'|b$.

$\boxed{\text{Debemos mostrar que } d'|d}$

En este momento conviene re_

cordar lo siguiente:

- estamos suponiendo que d cumple la Definición II
- usando la Definición II demostramos el Teorema III.

Esto significa que podemos aplicar el Teorema III y deducir que d es combinación lineal de a y b.

Así, $\exists\, \alpha, \beta \in \mathbb{Z}$ tales que

$$d = \alpha a + \beta b$$

Ahora recuerda qué estamos suponiendo de d'.

¿Te acuerdas?

Estamos suponiendo que

$$d' | a \quad y \quad d' | b.$$

Por el Lema de la combinación lineal obtenemos que $d' | \alpha a + \beta b$ es decir, $\boxed{d' | d}$

$\therefore$ d cumple 3) de la Definición IV

$\therefore$ d cumple la Definición IV.

$\Leftarrow$) Supongamos ahora que d cumple la Definición IV.

$\boxed{\text{P.D. d cumple la Definición II.}}$

Como d cumple 2) de la Definición IV, entonces d cumple i) de la Definición II.

Para ver que d cumple ii) de la Definición II, sea $d' \in \mathbb{Z}$ y supongamos que

$$d' | a \quad y \quad d' | b$$

$\boxed{\text{P.D. } d' \leq d}$

Aplicando 3) de la Definición IV sabemos que $d' | d$.

Ahora, puedes aplicar aquí

el Lema #?
(¿qué dice el famoso Lema #?)
Por i) de la Definición IV se tiene que $d \neq 0$, así que el Lema # garantiza que

$$|d'| \leq |d|.$$

Usando una vez más que d cumple i) de la Definición IV, se sigue que $|d| = d$.

En consecuencia,

$$d' \leq |d'| \leq |d| = d$$

y así, $d' \leq d$.

$\therefore$ d cumple ii) de la Definición II

$\therefore$ d cumple la Definición II.

$\square$