Máximo común divisor

$a, b \in \mathbb{Z} \quad b \neq 0$

$\operatorname{mcd}(a,b) = \max\{x \in \mathbb{Z} : x|a \text{ y } x|b\}$

Ejercicio 2. [Algoritmo de Euclides]. Sean $a, b \in \mathbb{Z}$.

a. Probar que si $d|a$ y $d|b$, entonces $d|(ax+by)$, para todo $x, y \in \mathbb{Z}$.

b. Probar que $\operatorname{mcd}(a,b) = \operatorname{mcd}(b, a-bq)$, para todo $q \in \mathbb{Z}$.

c. Describir el Algoritmo de Euclides para calcular el $\operatorname{mcd}(a,b)$.

d. Usar el Algoritmo de Euclides para calcular el $\operatorname{mcd}(a,b)$ en los siguientes casos:

i) $a = 63,\ b = 15$. ii) $a = 455,\ b = 1235$. iii) $a = 2366,\ b = 273$.

a) $d|a$ y $d|b \Rightarrow \underbrace{d|ax+by}$ para todo $x, y \in \mathbb{Z}$

$ax + by = dQ$ para algún $Q \in \mathbb{Z}$

$d|a \Rightarrow a = dq$ para algún $q \in \mathbb{Z}$

$d|b \Rightarrow b = dq'$ para algún $q' \in \mathbb{Z}$

$a = dq \Rightarrow ax = dqx$

$b = dq' \Rightarrow by = dq'y$

$ax + by = dqx + dq'y$

Entonces:

$$ax + by = dqx + dq'y = d\underbrace{(qx + q'y)}_{\in \mathbb{Z}}$$

$\Rightarrow d|ax+by$

b) $\operatorname{mcd}(a,b) = \operatorname{mcd}(b, a-bq)$ para todo $q \in \mathbb{Z}$

$d = \operatorname{mcd}(a,b) = \max\{x \in \mathbb{Z} : x|a \text{ y } x|b\}$

$d' = \operatorname{mcd}(b, a-bq) = \max\{x \in \mathbb{Z} : x|b \text{ y } x|a-bq\}$

queremos ver que $d = d'$

$*\ d \leq d'$

<u>idea</u>: ver que $d \in \{x \in \mathbb{Z} : x|b \text{ y } x|a-bq\}$

entonces como $d' = \max\{x \in \mathbb{Z} : x|b \text{ y } x|a-bq\}$

vamos a poder concluir que $d \leq d'$

vamos a probar que $d \in \{x \in \mathbb{Z} : x|b \text{ y } x|a-bq\}$

$d = \operatorname{mcd}(a,b) \Rightarrow \begin{cases} d|a \\ d|b \end{cases} \Rightarrow \begin{cases} d|b \\ d|a-bq \end{cases} \Leftarrow$ por la parte a) entonces $d \in \{x \in \mathbb{Z} : x \mid b \text{ y } x \mid a-bq\}$

$\Rightarrow d \leq d'$ porque $d' = \max\{x \in \mathbb{Z} : x \mid b \text{ y } x \mid a-bq\}$

* $d' \leq d$

vamos a probar que $d' \in \{x \in \mathbb{Z} : x \mid a \text{ y } x \mid b\}$

$$d' = mcd(b, a-bq) \Rightarrow \begin{cases} d' \mid b \\ d' \mid a-bq \end{cases}$$

$$\Rightarrow \begin{cases} d' \mid b \\ d' \mid (a-bq)+bq \end{cases} \leftarrow \text{por la parte a)}$$

$$\Rightarrow \begin{cases} d' \mid b \\ d' \mid a \end{cases}$$

$\Rightarrow d' \in \{x \in \mathbb{Z} : x \mid b \text{ y } x \mid a\}$

$\Rightarrow d' \leq d$ porque $d = \max\{x \in \mathbb{Z} : x \mid a, x \mid b\}$

c) <u>Algoritmo de Euclides</u>

Suponemos $a > b$

teorema de la división entera

① $a = \underline{b}q_1 + \underline{r_1}$ $\rightsquigarrow mcd(a,b) = mcd(b, a-bq_1) = mcd(b, r_1)$

$0 < r_1 < b$
$r_1 = a - bq_1$

② $b = \underline{r_1} q_2 + \underline{r_2}$ $\rightsquigarrow mcd(b, r_1) = mcd(r_1, b - r_1 q_2) = mcd(r_1, r_2)$

$0 < r_2 < r_1$
$r_2 = b - r_1 q_2$

③ $r_1 = \underline{r_2} q_3 + \underline{r_3}$ $\rightsquigarrow mcd(r_1, r_2) = mcd(r_2, r_3)$

$\vdots$

$mcd(r_n, 0) = r_n$

d) $\text{mcd}(1235, 455) = ?$

$1235 = \underline{455} \cdot 2 + \underline{325} \quad \rightarrow \text{mcd}(1235, 455) = \text{mcd}(455, 325)$

$455 = \underline{325} \cdot 1 + \underline{130} \quad \rightarrow \text{mcd}(455, 325) = \text{mcd}(325, 130)$

$325 = \underline{130} \cdot 2 + \underline{65} \quad \rightarrow \text{mcd}(325, 130) = \text{mcd}(130, 65)$

$130 = 65 \cdot 2 + \underline{0} \quad \rightarrow \text{mcd}(130, 65) = \text{mcd}(65, 0) = 65$

$\text{mcd}(1235, 455) = 65$

Teorema (Igualdad de Bezout)

$a, b \in \mathbb{Z}, \; a, b \neq 0$

① $\text{mcd}(a,b) = \min\{s > 0 : s = au + bv \text{ con } u, v \in \mathbb{Z}\}$

② en particular existen $x, y \in \mathbb{Z}$ tales que $\text{mcd}(a,b) = ax + by$

Decimos que $a, b \in \mathbb{Z}$ son coprimos si $\text{mcd}(a,b) = 1$

a y b son coprimos $\iff$ existen $x, y \in \mathbb{Z}$ tales que $ax + by = 1$

Ejercicio 3. [Lema de Euclides]. Sean $a, b, c \in \mathbb{N}$, tales que $\boxed{\text{mcd}(a, b) = 1}$ (a y b son primos entre sí). Probar o dar un contraejemplo de las siguientes afirmaciones.

a. Si $a|(bc)$ entonces $a|c$.

b. Si $a|c$ y $b|c$ entonces $ab|c$.

c. ¿Valen las partes anteriores si $\text{mcd}(a, b) \neq 1$?

a) $\left.\begin{array}{l} \text{mcd}(a,b) = 1 \\ a | bc \end{array}\right] \Rightarrow \underbrace{a|c}_{c = a\underbrace{(\cdots)}_{\in \mathbb{Z}}}$

* $\text{mcd}(a,b) = 1 \Rightarrow$ existen $x, y \in \mathbb{Z}$ tales que $ax + by = 1$
* $a | bc \Rightarrow bc = aq$ para algún $q \in \mathbb{Z}$

$$ax + by = 1 \Rightarrow acx + bcy = c$$
$$\Rightarrow acx + aqy = c$$
$$\Rightarrow a\underbrace{(cx + qy)}_{\in \mathbb{Z}} = c$$

entonces $a | c$

b) $\left.\begin{array}{l} \text{mcd}(a,b)=1 \\ a|c \text{ y } b|c \end{array}\right] \Rightarrow ab|c$

$$ab\underbrace{(\ldots)}_{\in\mathbb{Z}} = c$$

$*$ $\text{mcd}(a,b)=1 \Rightarrow$ existen $x,y\in\mathbb{Z}$ tales que $ax+by=1$

$*$ $a|c \Rightarrow c=aq$ para algún $q\in\mathbb{Z}$

$*$ $b|c \Rightarrow c=bq'$ para algún $q'\in\mathbb{Z}$

$$ax+by=1 \Rightarrow acx+bcy=c$$
$$\Rightarrow abq'x+baqy=c$$
$$\Rightarrow ab\underbrace{(q'x+qy)}_{\in\mathbb{Z}}=c$$

entonces $ab|c$.

Ejercicio 4. [Bezout] Sean $a,b,c\in\mathbb{N}$. Probar las siguientes afirmaciones:

a. $\text{mcd}(ca,cb)=c\,\text{mcd}(a,b)$. Sugerencia: usar Bezout y probar la doble desigualdad.

b. Si $c|a$ y $c|b$ entonces: $\text{mcd}(a/c,b/c)=\text{mcd}(a,b)/c$.

c. Si a y b son primos entre sí, entonces: $\text{mcd}(a-b,a+b)=1$ o 2. Sugerencia: probar primero que $\text{mcd}(a-b,a+b)$ divide a $\text{mcd}(2a,2b)$.

$a,b,c\in\mathbb{N}$

a) $\text{mcd}(ca,cb)=c\,\text{mcd}(a,b)$

$\text{mcd}(ca,cb)=cax+cby$

$\text{mcd}(a,b)=ax'+by'$

$c\,\text{mcd}(a,b)=cax'+cby'$

$*$ $\text{mcd}(ca,cb)\geq c\,\text{mcd}(a,b)$

por Bezout, existen $x,y\in\mathbb{Z}$ tales que

$$\text{mcd}(ca,cb)=cax+cby$$
$$=c(ax+by)$$

$ax+by\in\{s>0 : au+bv \text{ con } u,v\in\mathbb{Z}\}$

entonces como $\text{mcd}(a,b)=\min\{s>0 : au+bv \text{ con } u,v\in\mathbb{Z}\}$

concluimos que

$$ax+by\geq\text{mcd}(a,b)$$

Entonces:

$$\begin{aligned} mcd(ca, cb) &= cax + cby \\ &= c(ax + by) \\ &\geq c\, mcd(a,b) \end{aligned}$$

* $c\, mcd(a,b) \geq mcd(ca, cb)$

por Bezout, existen $x, y \in \mathbb{Z}$ tales que

$$mcd(a,b) = ax + by$$

$$\begin{aligned} c\, mcd(a,b) &= c(ax + by) \\ &= cax + cby \end{aligned}$$

$cax + cby \in \{ s > 0 : s = cau + cbv \text{ con } u, v \in \mathbb{Z} \}$

entonces como $mcd(ca, cb) = \min \{ s > 0 : s = cau + cbv \text{ con } u, v \in \mathbb{Z} \}$

concluimos que

$$cax + cby \geq mcd(ca, cb)$$

Entonces:

$$\begin{aligned} c\, mcd(a,b) &= c(ax + by) \\ &= cax + cby \\ &\geq mcd(ca, cb) \end{aligned}$$