Máximo común divisor

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

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

Ejercicio 1. [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 $\text{mcd}(a,b) = \text{mcd}(b, a-bq)$, para todo $q \in \mathbb{Z}$.

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

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

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

a) si $d|a$ y $d|b$ entonces $d|ax+by$

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

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

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

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

entonces $d|ax+by$

b) Queremos ver que $\text{mcd}(a,b) = \text{mcd}(b, a-bq)$ para todo $q \in \mathbb{Z}$

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

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

* $d \leq d'$

idea: ver que $d \in \{x \in \mathbb{Z} : x|b, x|a-bq\}$

$$d = \text{mcd}(a,b) \Rightarrow \begin{cases} d|a \\ d|b \end{cases}$$

$$= \begin{cases} d|a-bq \leftarrow \text{por la parte a)} \\ d|b \end{cases}$$

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

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

→ $d' \leq d$

idea: ver que $d' \in \{x \in \mathbb{Z} : x|a \text{ y } x|b\}$

$d' = mcd(b, a-bq) \Rightarrow \begin{cases} d'|b \\ d'|a-bq \end{cases}$ $\quad \underbrace{a-bq}_{} + \underbrace{bq}_{} = a$

$\Rightarrow \begin{cases} d'|b \\ d'|1(a-bq)+qb \end{cases}$ ← por la parte a)

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

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

c) Algoritmo de Euclides

PARTE B:
$mcd(a,b) = mcd(b, a-bq)$

$mcd(a,b) = ?$

suponemos que $a > b$

① $a = bq_1 + r_1 \rightarrow r_1 = a - bq_1$ $\quad \rightarrow mcd(a,b) = mcd(b, a-bq_1) = mcd(b, r_1)$

② $b = r_1 q_2 + r_2 \rightarrow r_2 = b - r_1 q_2$ $\quad \rightarrow mcd(b, r_1) = mcd(r_1, b - r_1 q_2) = mcd(r_1, r_2)$

③ $r_1 = r_2 q_3 + r_3$ $\quad \rightarrow mcd(r_1, r_2) = mcd(r_2, r_3)$

$\vdots$

$= mcd(r_n, 0) = r_n$

d) $mcd(63,15) = ?$

$63 = 15 \cdot 4 + 3$ $\quad \rightarrow mcd(63,15) = mcd(15,3)$

$15 = 3 \cdot 5 + 0$ $\quad \rightarrow mcd(15,3) = mcd(3,0) = 3$

Entonces $mcd(63,15) = 3$

Teorema: Igualdad de Bezout

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

① $\mathrm{mcd}(a,b) = \min\{s > 0 : s = ax + by \text{ con } x, y \in \mathbb{Z}\}$

② en particular existen $u, v \in \mathbb{Z}$ tales que $\mathrm{mcd}(a,b) = au + bv$

Decimos que a y b son coprimos si $\mathrm{mcd}(a,b) = 1$

a y b son coprimos $\Leftrightarrow$ existen $u, v \in \mathbb{Z}$ tales que $au + bv = 1$

Ejercicio 2. [Lema de Euclides]. Sean $a, b, c \in \mathbb{N}$, tales que $\mathrm{mcd}(a, b) = 1$ (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 $\mathrm{mcd}(a, b) \neq 1$?

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

$\mathrm{mcd}(a,b) = 1$

Queremos probar que si $a|bc$ entonces $a|c$ ($c = aQ$ con $Q \in \mathbb{Z}$)

* $a|bc \Rightarrow bc = aq$ para algún $q \in \mathbb{Z}$
* $\mathrm{mcd}(a,b) = 1 \Rightarrow$ existen $u, v \in \mathbb{Z}$ tales que $au + bv = 1$

$$au + bv = 1 \Rightarrow acu + bcv = c$$
$$\Rightarrow acu + aqv = c$$
$$\Rightarrow a\underbrace{(cu + qv)}_{\in \mathbb{Z}} = c$$

entonces $a|c$

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

$\rightarrow \mathrm{mcd}(a,b) = 1$

Queremos probar que si $a|c$ y $b|c$ entonces $ab|c$ ($c = Qab$ para algún $Q \in \mathbb{Z}$)

* $a|c \Rightarrow c = aq$ con $q \in \mathbb{Z}$
* $b|c \Rightarrow c = bq'$ con $q' \in \mathbb{Z}$

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

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

Entonces $ab|c$

Ejercicio 3. Sean $a, b, c \in \mathbb{N}$. Probar las siguientes afirmaciones:

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

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

c. Si a y b son primos entre sí, entonces: $\mathrm{mcd}(a - b, a + b) = 1$ o 2.

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

Queremos ver que $\mathrm{mcd}(ca, cb) = c\,\mathrm{mcd}(a, b)$

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

existen enteros x, y tales que $\mathrm{mcd}(ca, cb) = cax + cby$

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

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

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

por lo tanto $ax + by \geq \mathrm{mcd}(a,b)$

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

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

Por la igualdad de Bezout existen $x, y \in \mathbb{Z}$ tales que $\mathrm{mcd}(a,b) = ax + by$

$$c\,mcd(a,b) = c(ax+by)$$
$$= cax + cby$$

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

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

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

$$c\,mcd(a,b) = c(ax+by)$$
$$= cax + cby$$
$$\geq mcd(ca, cb)$$

c. Si a y b son primos entre sí, entonces: $\mathrm{mcd}(a-b, a+b) = 1$ o 2.

veamos que el mayor divisor comun de $a-b$ y $a+b$ es 1 o 2

Sea $x \in \mathbb{N}$ tal que

$$\begin{cases} x \mid a-b \\ x \mid a+b \end{cases}$$

entonces $x \mid (a-b)+(a+b)$ es decir $x \mid 2a$

$x \mid (a+b)-(a-b)$ es decir $x \mid 2b$

$x \mid 2a$ y $x \mid 2b \Rightarrow x \mid mcd(2a, 2b)$

$mcd(2a, 2b) = \underline{2a}u + \underline{2b}v$

$x \mid mcd(2a, 2b) \Rightarrow x \mid 2\underbrace{mcd(a,b)}_{=1}$

$\Rightarrow x \mid 2$

$\Rightarrow x = 1$ o $x = 2$