Apuntes sobre Divisibilidad

September 2024

1 Teorema de la división Euclidea

Sean $a, b \in \mathbb{Z}$, con $b \neq 0$. Entonces, $\exists! q, r \in \mathbb{Z}$, tales que $a = bq + r$, con $0 \leq r < |b|$.

2 Definición

Dados $a, b \in \mathbb{Z}$, decimos que $d = mcd(a, b)$ si:

- $d > 0$
- $d|a$ y $d|b$
- Si $d'|a$ y $d'|b$ entonces $d'|d$

3 Teorema

Si $a \neq 0$ ó $b \neq 0$, entonces $\exists! d = mcd(a, b)$

3.1 Demostración

Consideremos el conjunto $\Delta = \{ax + by > 0 : x, y \in \mathbb{Z}\}$. Veamos que $d = min(\Delta) = mcd(a, b)$. En primer lugar, constatamos que existe el minimo de este conjunto, ya que $\Delta \neq \emptyset$. Efectivamente, basta con tomar $x = a$, $y = b$, con lo que $0 < a^2 + b^2 \in \Delta$.

- Por definición, $d > 0$
- Veamos que $d|a$. Expresamos $d = ax_o + by_o$. Entonces, por el teorema de la división euclidea, $r = a - dq$ con $0 \leq r < d$, lo cual podemos reescribir como $r = a - (ax_o + by_o)q = a(1 - qx_o) + b(-qy_o)$. Si $r > 0$, entonces $r \in \Delta$, pero $r < d = min(\Delta)$, luego tenemos que conluir que $r = 0$. Por simetría, tendremos que $d|b$.

- Finalmente, veamos que se $d'|a$ y $d'|b$ entonces $d'|d$. Efectivamente, consideremos:

$$\begin{cases} d'|a \Rightarrow a = d'a' \\ d'|b \Rightarrow ab = d'b' \\ d = ax_o + by_o \end{cases} \quad (1)$$

De lo anterior se concluye que $d = d'a'x_o + d'b'y_o = d'(a'x_o + b'y_o)$. Esto es $d|d'$ □

4 Teorema del algoritmo de Euclides

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$, y sea $a = bq + r$ con $0 \leq r < |b|$ y $r, q \in \mathbb{Z}$. Entonces, $mcd(a, b) = mcd(b, r)$

4.1 Demostración

Sea $d = mcd(a, b)$. Entonces $d|a$ y $d|b$. Esto es, $\exists a', b' \in \mathbb{Z}$ tales que $a = da'$ y $b = db'$. Por tanto, $r = a - bq = da' - db'q = d(a' - b'q)$, por lo que $d|r$ (y $d|b$).

Por otro lado, si $d'|b$ y $d'|r$, entonces $\exists b', r' \in \mathbb{Z}$ con $b = b'd'$ y $r = r'd'$, con lo cual $a = bq + r = b'd'q + r'd' = d'(b'q + r')$ y así $d'|a$ (y $d'|b$). Por tanto, $d'|d$ ya que $d = mcd(b, r)$.

Finalmente, $d \geq 0$ por definición. Concluimos, pues, que $d = mcd(b, r)$ □