Matemática Discreta II

Mauro Polenta Mora

CLASE 3 - 20/08/2025

Máximo común divisor

Más corolarios 1.2.9

1

- Si $e \in \mathbb{Z}$ es tal que $e \mid a$ y $e \mid b$, entonces $e \mid mcd(a, b)$

Demostración:

Directa por Bezout.

2

- $mcd(a, b) = 1 \iff \exists x, y \in \mathbb{Z}$ tal que $ax + by = 1$

Demostración:

Llamamos $d = mcd(a, b)$

El directo es inmediato por Bezout. Para el recíproco observemos que por propiedades de divisibilidad tenemos:

- $d \mid a$ y $d \mid b$ entonces $d \mid ax + by$ para todo $x, y \in \mathbb{Z}$

Por lo tanto concluimos que:

- $d \mid ax + by = 1$, entonces
- $d \mid 1$

Y como el único divisor positivo de 1 es si mismo, tenemos que:

- $mcd(a, b) = d = 1$

3

- Si $n \in \mathbb{Z}$ entonces $mcd(na, nb) = |n|mcd(a, b)$

Demostración:

Para esta parte se asume que $n \in \mathbb{Z}^+$. La estrategia es probar que:

- $mcd(na, nb) \mid n \cdot mcd(a, b)$
- $n \cdot mcd(a, b) \mid mcd(na, nb)$

Llamamos:

- $d = mcd(a, b)$, y
- $d' = mcd(na, nb)$

Veamos las dos pruebas que queremos hacer:

$d' \mid (n \cdot d)$:

Por Bézout tenemos que $d = ax + by$, veamos el siguiente razonamiento:

$$
\begin{aligned}
& d = ax + by \\
& \iff \text{(multiplico por } n\text{)} \\
& nd = nax + nby \\
& \iff (na = d'q_1; nb = d'q_2) \\
& nd = d'q_1x + d'q_2y \\
& \iff \\
& nd = d'(q_1x + q_2y) \\
& \iff \\
& n \cdot mcd(a, b) = d'(q_1x + q_2y)
\end{aligned}
$$

Por lo tanto tenemos que $d' \mid (n \cdot d)$.

$(n \cdot d) \mid d'$**:**

Como $d = mcd(a, b)$, tenemos que:

$$
\begin{aligned}
& \begin{cases} d \mid a \\ d \mid b \end{cases} \\
& \Rightarrow \text{(por propiedades de divisibilidad)} \\
& \begin{cases} nd \mid na \\ nd \mid nb \end{cases}
\end{aligned}
$$

Entonces $nd \mid mcd(na, nb)$, es decir que $nd \mid d'$

Entonces juntando ambas partes podemos concluir que:

$d = d'$

Lo que concluye la prueba.

4

Si $d \in \mathbb{Z}^+$ tal que $a = da^*$ y $b = db^*$ con $a^*, b^* \in \mathbb{Z}$. Entonces $d = mcd(a, b) \iff mcd(a^*, b^*) = 1$.

A los enteros a^* y b^* tales que $a = mcd(a,b)a^*$ y $b = mcd(a,b)b^*$ se les llama cofactores de a y b.

Demostración:

Veamos el siguiente razonamiento:

$$\begin{aligned} & d \\ & = \\ & mcd(a,b) \\ & = \\ & mcd(da^*, db^*) \\ & =_{\text{(por el corolario anterior)}} \\ & d \cdot mcd(a^*, b^*) \end{aligned}$$

Por lo tanto $mcd(a^*, b^*) = 1$ para satisfacer la igualdad.

Lema de Euclides 1.2.10

Otro corolario pero más importante es el siguiente.

Sean $a, b, c \in \mathbb{Z}$ con $mcd(a,b) = 1$. Si $a \mid bc$ entonces $a \mid c$.

Demostración:

Por la igualdad de Bézout sabemos que:

- $\exists x, y \in \mathbb{Z} : ax + by = 1$, si multiplicamos por c obtenemos:
- $c = cax + cby$

Observemos que por hipótesis tenemos que:

$$\begin{cases} a \mid a \\ a \mid bc \end{cases}$$

A partir de esto, por propiedades de divisibilidad:

- $a \mid (cx)a + (cb)y = c$

Por lo que esto demuestra la propiedad.

Corolario 1.2.11

Sea p un entero primo y $b, c \in \mathbb{Z}$. Si $p \mid bc$ entonces $p \mid b$ o $p \mid c$.

Demostración:

Distinguimos dos casos:

- $p \mid b$: Directo, la propiedad se cumple
- $p \nmid b$: Sabemos que:

- $p \mid bc$ por hipótesis
- $mcd(p, b) = 1$ por p primo

Entonces usando el Lema de Euclides concluimos que:

- $p \mid c$

Por lo tanto en cualquiera de los casos se cumple la propiedad.

Observación 1.2.13

Esta propiedad se generaliza para n enteros de la siguiente forma:

Sea p un entero primo y $a_1, \dots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \dots a_n$, entonces $p \mid a_i$ para algún $i \in \{1, \dots, n\}$.

Definición 1.2.14 (mínimo común múltiplo)

Dados $a, b \in \mathbb{Z}$ no nulos, definimos el mínimo común múltiplo de a y b como:

- $mcm(a, b) = \min\{x \in \mathbb{Z}^+ : a \mid x \text{ y } b \mid x\}$

En el caso de que alguno sea nulo (por ejemplo $a = 0$) lo definimos por:

- $mcm(0, b) = 0 \quad \forall b \in \mathbb{Z}$

De la misma forma que para el máximo común divisor, nos interesa tener un algorítmo para hallar el mínimo común múltiplo sin tener que conocer todos sus divisores o múltiplos.

Proposición 1.2.15

Dados $a, b \in \mathbb{Z}$ no nulos, se cumple que:

- $mcm(a, b) = \frac{|ab|}{mcd(a,b)}$

Demostración

Llamamos $m = mcm(a, b)$ y $d = mcd(a, b)$, también consideramos a, b positivos para la prueba y por tanto queremos probar que:

- $m = \frac{ab}{d}$

La estrategia será probar desigualdad de ambos lados:;

- $m \leq \frac{ab}{d}$
- $\frac{ab}{d} \leq m$

$m \leq \frac{ab}{d}$:

Observemos que:

- $\frac{ab}{d} = a(\frac{b}{d}) = \dot{a}$, pues $\frac{b}{d} \in \mathbb{Z}$
- $\frac{ab}{d} = b(\frac{a}{d}) = \dot{b}$, pues $\frac{b}{d} \in \mathbb{Z}$

Juntando las dos afirmaciones, tenemos que:

- $m \leq \frac{ab}{d}$, pues m es el mínimo común múltiplo entre a y b.

$\frac{ab}{d} \leq m$:

Como a, b son múltiplos de m, podemos decir que existen $x, y \in \mathbb{Z}^+$ (no nulos pues a, b son no nulos y positivos pues a, b son positivos) tales que:

- $m = ax$
- $m = by$

Por otra parte, por Bézout tenemos que existen $x', y' \in \mathbb{Z}^+$ (positivos pues a, b positivos) tales que:

- $ax' + by' = d$

Operemos con esta expresión:

$$\begin{aligned} & ax' + by' = d \\ & \iff \text{(multiplico ambos lados por } xy \neq 0) \\ & axyx' + byxy' = dxy \\ & \iff (ax = by = m) \\ & myx' + mxy' = dxy \quad (*_1) \end{aligned}$$

Ahora, observemos este otro razonamiento:

$$\begin{aligned} & m^2 = abxy \\ & \iff \text{(multiplico por } \tfrac{d}{d} = 1) \\ & m^2 = \frac{ab}{d} dxy \\ & \iff (dxy = m(yx' + xy')) \\ & m^2 = \frac{ab}{d} m(yx' + xy') \\ & \iff \text{(llamando } z = (yx' + xy') \text{ y dividiendo por } m \neq 0) \\ & m = \frac{ab}{d} z \end{aligned}$$

Como $z \geq 1$, pues $x, y, x', y' \in \mathbb{Z}^+$, se tiene que:

- $\frac{ad}{b} \leq m$

Juntando ambas partes, se puede concluir que:

- $\frac{ad}{b} = m$

Lo que demuestra la propiedad.

Algunas observaciones

- Análogamente a cómo lo hicimos anteriormente para dos enteros, podemos definir el máximo común divisor de cualquier cantidad de enteros.
  - Dados $a_1, \ldots, a_n \in \mathbb{Z}$, con $n > 2$, no todos nulos, se define:

$$* \ mcd(a_1, ..., a_n) = max\{x \in \mathbb{Z} : x \mid a_i, \forall i = 1, ..., n\}$$

- $mcd(a_1, a_2, ..., a_n) = mcd(mcd(a_1, a_2, ..., a_{n-1}), a_n)$
- En consecuencia a esto último, es posible probar por inducción una igualdad de Bézout generalizada: Existen enteros $x_1, x_2, ..., x_n$ tales que:
  - $a_1x_1 + a_2x_2 + ... + a_nx_n = mcd(a_1, a_2, ..., a_n)$

Pruebas de irracionalidad

Como consecuencia del Lema de Euclides, podemos probar que $\forall p$ primo, $\sqrt{p}$ es irracional. Veámoslo.

Proposición 1.3.1

$\forall p$ primo, $\sqrt{p}$ no es racional.

Demostración

Supongamos por absurdo que $\sqrt{p}$ es racional, entonces:

- $\sqrt{p} = \frac{a}{b}$ con $a, b \in \mathbb{Z}^+$, y
- $mcd(a, b) = 1$

Entonces, se tiene que:

$$\begin{aligned}
&\sqrt{p} = \frac{a}{b} \\
&\iff \\
&b\sqrt{p} = a \\
&\iff \\
&b^2p = a^2 \\
&\iff \\
&p \mid a^2 \\
&\iff \text{(por los corolarios del Lema de Euclides)} \\
&p \mid a
\end{aligned}$$

A partir de esto, consideremos $a' \in \mathbb{Z}^+$ tal que $a = pa'$. Volviendo a la igualdad $b^2p = a^2$ tenemos que:

$$
\begin{aligned}
& b^2p = a^2 \\
& \quad \iff \\
& b^2p = p^2(a')^2 \\
& \quad \iff \text{(dividiendo por } p{\neq}0\text{)} \\
& b^2 = p(a')^2 \\
& \quad \iff \\
& p \mid b^2 \\
& \quad \iff \text{(por los corolarios del Lema de Euclides)} \\
& p \mid b
\end{aligned}
$$

Pero esto es absurdo, pues $p \mid a$ y $p \mid b$, y nosotros consideramos $mcd(a, b) = 1$.

Esto concluye la prueba.