Taller 1 - Teoría de Números

Christian Mauricio Cárdenas Barón

20251167009

Carlos Andres Giraldo Hernandez

Facultad de Ciencias Matemáticas y Naturales

Universidad Distrital Francisco José de Caldas

2025-10-02

1. Taller

1. Demuestre por inducción:

$$a_1|a_2, a_2|a_3, ..., a_{n-1}|a_n \implies a_1|a_n$$

Demostración:

- Caso Base: $n = 3$

  Por hipótesis $a_1|a_2$ y $a_2|a_3$, existen $x, y \in \mathbb{Z}$ tal que $a_2 = a_1x$ y $a_3 = a_2y$

  $$a_3 = a_2y = (a_1x)y = a_1(xy) \implies a_1|a_3$$

- Paso inductivo: Supongamos $a_1|a_2, a_2|a_3, ..., a_{n-1}|a_n \implies a_1|a_n$

  También se supone la relación para $n + 1$ tal que

  $$a_1|a_2, a_2|a_3, ...a_{n-1}|a_n, a_n|a_{n+1}$$

  Por HI $a_1|a_n$ y $a_n|a_{n+1}$, existen $x, y \in \mathbb{Z}$ tal que $a_n = a_1x$ y $a_{n+1} = a_ny$

  $$a_{n+1} = a_ny = (a_1x)y = a_1(xy) \implies a_1|a_{n+1}$$

□

2. Demuestre por inducción:

$$a|b_1, a|b_2, ..., a|b_n \implies a|(b_1x_1 + b_2x_2 + ... + b_nx_n), \quad x_1, x_2, ..., x_n \in \mathbb{Z}$$

Demostración:

- Caso base: $n = 2$

  Por definición existen $y_1, y_2 \in \mathbb{Z}$ tal que $b_1 = ay_1$ y $b_2 = ay_2$

  Multiplicando por sus respectivos x_i

  $$\begin{array}{rr} b_1 = ay_1 & b_2 = ay_2 \\ b_1x_1 = ay_1x_1 & b_2x_2 = ay_2x_1 \end{array}$$

  Sumando las expresiones

  $$b_1x_1 + b_2x_2 = ay_1x_1 + ay_2x_2$$
  $$b_1x_1 + b_2x_2 = a(y_1x_1 + y_2x_2)$$

  Por lo tanto $a|(b_1x_1 + b_2x_2)$

- Paso Inductivo: Supongamos

  $$a|b_1, a|b_2, ..., a|b_n \implies a|(b_1x_1 + b_2x_2 + ... + b_nx_n), \quad x_1, x_2, ..., x_n \in \mathbb{Z}$$

  También se supone la relación para $n + 1$, tal que $a|b_{n+1}$

  Por HI $b_1x_1 + b_2x_2 + ... + b_nx_n = ak, \quad k \in \mathbb{Z}$

  Como $a|b_{n+1}$, entonces $b_{n+1} = aq, \quad q \in \mathbb{Z}$

$$\begin{aligned} b_1x_1 + b_2x_2 + ... + b_nx_n + b_{n+1}x_{n+1} &= ak + b_{n+1}x_{n+1} \\ &= ak + (aq)x_{n+1} \\ &= a(k + qx_{n+1}) \end{aligned}$$

Por lo tanto $a|(b_1x_1 + b_2x_2 + ... + b_nx_n + b_{n+1}x_{n+1})$

$\square$

3. Demostrar por inducción: Sean $a_1, a_2, ..., a_n \in \mathbb{Z}$ no nulos simultáneamente, existen enteros $x_1, x_2, ..., x_n$, tales que

$$(a_1, a_2, ..., a_n) = a_1x_1 + a_2x_2 + ... + a_nx_n$$

Demostración:

- Caso Base: $n = 2$

  Sea $S = \{a_1x + a_2y : x, y \in \mathbb{Z} \wedge a_1x + a_2y > 0\}$

  - Si $a_1 = a_2$ y $a_1 > 0$, entonces $a_1(1) + a_2(1) \in S$
  - Si $a_1 = a_2$ y $a_1 < 0$, entonces $a_1(-1) + a_2(-1) \in S$
  - Si $a_1 < a_2$, entonces $a_2 - a_1 > 0$, por lo tanto $a_1(-1) + a_2(1) \in S$
  - Si $a_1 > a_2$, entonces $a_1 - a_2 > 0$, por lo tanto $a_1(1) + a_2(-1) \in S$

  Entonces $S \neq \varnothing$

  Como $\min(S) \in S$, existen x_0, y_0 tal que

  $$\min(S) = a_1x_0 + a_2y_0$$

  $(a_1, a_2)|a_1 \wedge (a_1, a_2)|a_2 \implies (a_1, a_2)|(a_1x_0 + a_2 + y_0) \implies (a_1, a_2)|\min(S)$

  $(a_1, a_2)|\min(S) \wedge (a_1, a_2) > 0 \wedge \min(S) > 0 \implies (a_1, a_2) \leq \min(S)$

  Por algoritmo de la division existen únicos $q, r \in \mathbb{Z}$ tal que

  $$a_1 = \min(S)q + r, \quad 0 \leq r < \min(S)$$

  $$\begin{aligned} r &= a_1 - \min(S)q \\ &= a_1 - (a_1x_0 + a_2y_0)q \\ &= a_1 - a_1x_0q - a_2y_0q \\ &= a_1(1 - x_0q) + a_2(-y_0q) \end{aligned}$$

  Si $r > 0 \implies r \in S \implies r \geq \min(S)$, lo cual contradice $r < \min(S)$

  Por lo tanto $r = 0 \implies a_1 = \min(S)q \implies \min(S)|a$

  «El razonamiento para $\min(S)|a_2$ es análogo»

  Como $\min(S)|a_1 \wedge \min(S)|a_2 \implies \min(S)|(a_1, a_2) \implies \min(S) \leq (a_1, a_2)$

  Por lo tanto $\min(S) \leq (a_1, a_2) \wedge (a_1, a_2) \leq \min(S) \implies \min(S) = (a_1, a_2)$

- Paso inductivo: Supongamos que para todo $a_1, a_2, ..., a_n \in \mathbb{Z}$ no nulos simultáneamente, existen $x_1, x_2, ..., x_n$ tales que

  $$(a_1, a_2, ..., a_n) = a_1x_1 + a_2x_2 + ... + a_nx_n$$

  Sea $d = (a_1, a_2, ..., a_n)$

  Por definición de MCD, d divide a cada $a_1, a_2, ..., a_n$

  - Sea c un divisor común de $a_1, a_2, ..., a_n, a_{n+1}$
    Como $d = (a_1, a_2, ..., a_n)$, entonces $c|d$
    Ademas $c|a_{n+1}$ por lo tanto c es divisor común de d, a_{n+1}
  - Recíprocamente. Sea c un divisor común de d, a_{n+1}
    Como $c|d$ y $d|a_1, d|a_2, ...d|a_n$, entonces $c|a_1, c|a_2, ..., c|a_n$
    Ademas $c|a_{n+1}$ por lo tanto c es divisor común de $a_1, a_2, ..., a_n, a_{n+1}$

  Por lo tanto el conjunto de divisores comunes de $a_1, a_2, ..., a_n, a_{n+1}$ es igual que el conjunto de divisores comunes de d, a_{n+1} y por definición de MCD $(a_1, a_2, ..., a_n, a_{n+1}) = (d, a_{n+1})$

  Por HI existen $x_1, x_2, ..., x_n$ tal que $d = a_1x_1 + a_2x_2 + ... + a_nx_n$

  Por teorema de Bézout existen y_1, y_2 tal que

  $$\begin{aligned}(d, a_{n+1}) &= dy_1 + a_{n+1}y_2 \\ &= (a_1x_1 + a_2x_2 + ... + a_ny_n)y_1 + a_{n+1}y_2 \\ &= a_1x_1y_1 + a_2x_2y_1 + ... + a_nx_ny_1 + a_{n+1}y_2 \\ &= a_1(x_1y_1) + a_2(x_2y_1) + ... + a_n(x_ny_1) + a_{n+1}(y_2)\end{aligned}$$

  Por lo tanto $(a_1, a_2, ..., a_n, a_{n+1})$ se puede expresar como una combinación lineal.

$\square$

4. Demostrar: Sean $a, b \in \mathbb{Z}$ no nulos simultáneamente,

$$d = (a, b) \iff \begin{cases} d > 0 \\ d|a \wedge d|b \\ m|a \wedge m|b \implies m|d \end{cases}$$

Demostración:

- $\implies$
  1. Como 1 es divisor común para cualquier pareja de enteros, tenemos que $d \geq 1$, entonces $d > 0$
  2. Por definición de MCD $d|a$ y $d|b$
  3. Sea $m \in \mathbb{Z}$ tal que $m|a$ y $m|b$.

     Por teorema de Bézout, existen $x, y \in \mathbb{Z}$ tal que $d = (a, b) = ax + by$

     $$m|a \wedge m|b \implies m|ax + by \implies m|d$$

- $\Longleftarrow$

  Por hipótesis $d > 0$, $d|a$ y $d|b$

  Sea $k \in \mathbb{Z}$ tal que $k|a$ y $k|b$. Por hipótesis $k|d$

  1. Si $k < 0$: como $d > 0$, entonces $k < d$
  2. Si $k > 0$: como $k|d$, entonces $k \leq d$

  Por lo tanto $d = (a, b)$

$\square$

5. Demostrar:

$$m > 0 \Longrightarrow (ma, mb) = m(a, b)$$

Demostración:

Sea $S_1 = \{max + mby : x, y \in \mathbb{Z} \wedge max + mby > 0\}$

$$(ma, mb) = \min(S_1) = max_0 + mby_0 = m(ax_0 + by_0)$$

Como $m(ax_0 + by_0) > 0$ y $m > 0$, entonces $ax_0 + by_0 > 0$

Sea $S_2 = \{ax + by : x, y \in \mathbb{Z} \wedge ax + by > 0\}$

$$m(ax_0 + by_0) = m \min(S_2) = m(a, b)$$

Por lo tanto $(ma, mb) = m(a, b)$ $\square$

6. Demostrar:

$$d > 0 \wedge d|a \wedge d|b \Longrightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$$

Demostración:

Como $d|a$ y $d|b$, existen $m, n \in \mathbb{Z}$ tal que $a = dm$ y $b = dn$

Por teorema de Bézout existen $x, y \in \mathbb{Z}$ tal que $(a, b) = ax + by$

$$(a, b) = ax + by = dmx + dny = d(mx + ny)$$

Como $d > 0$ y $d|(a, b)$ podemos dividir la expresión por d

$$\frac{(a, b)}{d} = \frac{d(mx + ny)}{d} = mx + ny = (m, n) = \left(\frac{a}{d}, \frac{b}{d}\right)$$

Por lo tanto $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$ $\square$

7. Demostrar:

$$(a, m) = (b, m) = 1 \Longrightarrow (ab, m) = 1$$

Demostración:

Por teorema de Bézout existen $x, y, u, v \in \mathbb{Z}$ tal que $(a, m) = ax + my = 1$ y $(b, m) = bu + mv = 1$

$$\begin{aligned}
1 &= (ax + my)(bu + mv) \\
&= (ax)(bu) + (ax)(mv) + (my)(bu) + (my)(mv) \\
&= ab(xu) + m(axv + byu + myv) \\
&= ab(xu) + m(axv + y(bu + mv)) \\
&= ab(xu) + m(axv + y)
\end{aligned}$$

Como $ab(xu) + m(axv + y)$ es una combinación lineal de ab y m, por teorema de Bézout existe una combinación tal que $ab(xu) + m(axv + y) = (ab, m)$ □

8. Demostrar:

$$(a, b) = (b, a) = (-a, b) = (a, -b) = (-a, -b) = (a, b + ax), \quad x \in \mathbb{Z}$$

Demostración:

1. $(a, b) = (b, a)$

Sean $S_1 = \{x \in \mathbb{Z} : x|a\}$ y $S_2 = \{x \in \mathbb{Z} : x|b\}$

Entonces $\text{div}(a, b) = S_1 \cap S_2$, pero también $\text{div}(b, a) = S_2 \cap S_1$

$$\text{div}(a, b) = S_1 \cap S_2 = S_2 \cap S_1 = \text{div}(b, a)$$

2. $(a, b) = (-a, b) = (a, -b), (-a, -b)$

Por definición si $d|a$, existe $k \in \mathbb{Z}$ tal que $a = dk$, pero $-a = d(-k)$, entonces $d|(-a)$. Por lo tanto los divisores de a y $-a$ son iguales.

Por lo tanto $(a, b) = (-a, b)$, analógicamente $(a, b) = (a, -b)$, finalmente $(a, b) = (-a, -b)$

3. $(a, b) = (a, b + ax), \quad x \in \mathbb{Z}$

Sean $K_1 = \{k \in \mathbb{Z} : k|a \wedge k|b\}$ y $K_2 = \{k \in \mathbb{Z} : k|a \wedge k|(b + ax)\}$

- Sea $d \in K_1$, tal que $d|a$ y $d|b$. Como $d|a$, entonces $d|ax$. Como $d|b$ y $d|ax$, entonces $d|b + ax$
  Por lo tanto $d \in K_2$, así $K_1 \subseteq K_2$
- Recíprocamente. Sea $d \in K_2$ tal que $d|a$ y $d|(b + ax)$, de modo que $d|ax$ por lo tanto d divide a $(b + ax) + a(-x) = b$, entonces $d|b$
  Por lo tanto $d \in K_1$, así $K_2 \subseteq K_1$

Por lo tanto $K_1 = K_2$, entonces $(a, b) = (a, b + ax)$

□

9. Demostrar:

$$c|ab \wedge (c, b) = 1 \Longrightarrow c|a$$

Demostración:

Por teorema de Bézout existen $x, y \in \mathbb{Z}$ tal que $(c, b) = 1 = cx + by$

Por definición existe $k \in \mathbb{Z}$ tal que $ab = ck$

$$
\begin{aligned}
1 &= cx + by \\
a &= acx + aby \\
a &= acx + (ck)y \\
a &= c(ax + ky)
\end{aligned}
$$

Por lo tanto $c|a$ $\square$