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

2025-09-28

1. Taller

1. Demuestre por inducción:

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

   ***Demostración** (no inducción):*

   Por Hipótesis existen $x_1, x_2, ..., x_{n-1} \in \mathbb{Z}$ tal que:

$$\begin{aligned} a_2 &= a_1 x_1 \\ a_3 &= a_2 x_2 && = a_1 x_1 x_2 \\ &\vdots \\ a_n &= a_{n-1} x_{n-1} = a_1 x_1 x_2 \cdots x_{n-1} \end{aligned}$$

   Entonces podemos expresar $a_n = a_1 \prod_{i=1}^{n-1} x_i$

   Como $\prod_{i=1}^{n-1} x_i = x_1 x_2 \cdots x_{n-1} \in \mathbb{Z}$, entonces $a_1|a_n$ □

   ***Demostración** (inducción):*

   - Caso Base: $n = 2$, $a_1|a_2$
   - Paso inductivo: Supongamos que si $a_1|a_2, a_2|a_3, ..., a_{n-1}|a_n$, entonces $a_1|a_n$

     Por HI $a_1|a_n$ entonces $a_n = a_1 k_1$ para algún $k_1 \in \mathbb{Z}$

     Duda: Como $a_n|a_{n+1}$ entonces $a_{n+1} = a_n k_2$ para algún $k_2 \in \mathbb{Z}$

     $a_{n+1} = a_n k_2 = a_1 k_1 k_2 \implies a_1|a_{n+1}$

   Por lo tanto si $a_1|a_2, a_2|a_3, ..., a_{n-1}|a_n$ entonces $a_1|a_n$ □

2. Demuestre por inducción:

   Si $a|b_1, a|b_2, ..., a|b_n$, entonces $a|b_1 x_1 + b_2 x_2 + ... + b_n x_n, \quad x_1, x_2, ..., x_n \in \mathbb{Z}$

   Demostración:

   - Caso base: $n = 2$

$$\begin{aligned} b_1 = ak_1 \land b_2 = ak_2 &\implies b_1 x_1 = ak_1 x_1 \land b_2 x_2 = ak_2 x_2 \\ &\implies b_1 x_1 + b_2 x_2 = ak_1 x_1 + ak_2 x_2 \\ &\implies b_1 x_1 + b_2 x_2 = a(k_1 x_1 + k_2 x_2) \\ &\implies a|(b_1 x_1 + b_2 x_2) \end{aligned}$$

   - Paso Inductivo: Supongamos

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

     Por HI $b_1 x_1 + b_2 x_2 + ... + b_n x_n = \sum_{i=1}^{n} (b_i x_i) = ak, \quad k \in \mathbb{Z}$

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

$$
\begin{aligned}
ak &= \sum_{i=1}^{n} (b_i x_i) \\
ak + b_{n+1}x_{n+1} &= \sum_{i=1}^{n} (b_i x_i) + b_{n+1}x_{n+1} \\
ak + aqx_{n+1} &= \sum_{i=1}^{n+1} (b_i x_i) \\
a(k + qx_{n+1}) &= \sum_{i=1}^{n+1} (b_i x_i)
\end{aligned}
$$

Esto muestra que $a| \sum_{i=1}^{n+1} (b_i x_i)$

Por lo tanto si $a|b_1, a|b_2, ..., a|b_n$, entonces $a| \sum_{i=1}^{n} (b_i x_i)$ □

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:

$$(\forall a_1, a_2, ..., a_n \in \mathbb{Z})(\exists x_1, x_2, ..., x_n \in \mathbb{Z})\left((a_1, a_2, ..., a_n) = \sum_{i=1}^{n} (a_i x_i)\right)$$

- Caso Base: $n = 2$

  Sea $S = \{a_1x + a_2y : x, y \in \mathbb{Z} \wedge a_1x + a_2y > 0\}$
  - $a_1 = a_2 \wedge a_1 > 0 \Longrightarrow a_1(1) + a_2(1) \in S$
  - $a_1 = a_2 \wedge a_1 < 0 \Longrightarrow a_1(-1) + a_2(-1) \in S$
  - $a_1 < a_2 \Longrightarrow a_2 - a_1 > 0 \Longrightarrow a_1(-1) + a_2(1) \in S$

  «El razonamiento para $a_1 \geq a_2$ es análogo»

  Entonces $S \neq \varnothing$

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

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

  $(a_1, a_2)|a_1 \wedge (a_1, a_2)|a_2 \Longrightarrow (a_1, a_2)| \min(S)$

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

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

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

  $$
  \begin{aligned}
  r &= a_1 - \min(S)q \\
  &= a_1 - (a_1x_0 + a_2y_0)q \\
  &= a_1 - a_1qx_0 - a_2qy_0 \\
  &= a_1(1 - qx_0) + a_2(-qy_0)
  \end{aligned}
  $$

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

$$(\forall a_1, a_2, ..., a_n \in \mathbb{Z})(\exists x_1, x_2, ..., x_n \in \mathbb{Z})\left((a_1, a_2, ..., a_n) = \sum_{i=1}^{n}(a_i x_i)\right)$$

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

$$g = \sum_{i=1}^{n}(a_i x_i)$$
$$g + a_{n+1}x_{n+1} = \sum_{i=1}^{n}(a_i x_i) + a_{n+1}x_{n+1}$$

Incompleta

□

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

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

Demostración:

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

  Sea $S = \{x \in \mathbb{Z} : x|a \wedge x|b\}$

  1. Por definición si $d = (a, b)$, entonces $d = \max(S)$, por lo tanto $d|a \wedge d|b$
  2. Si $m|a \wedge m|b \implies m \in S$, como $d = \max(S)$, entonces $m \leq d$

- $\left.\begin{matrix} d|a \wedge d|b \\ m|a \wedge m|b \implies m|d \end{matrix}\right\} \implies d = (a, b)$

  DUDA: Sea $a = 90 \wedge b = 60$

$$\operatorname{div}(90) = \{1, 2, 3, 5, 6, 9, 10, 15, 30, 45, 90\}$$
$$\operatorname{div}(60) = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$$
$$\operatorname{div}(90, 60) = \{1, 2, 3, 5, 6, 10, 15, 30\}$$

  Si tomamos $m = 2 \wedge d = 10$

$$10|90 \wedge 10|60$$
$$2|90 \wedge 2|60 \implies 2|10$$

  Pero $10 = d \neq (90, 60) = 30$

□

5. Demostrar: $m > 0 \implies (ma, mb) = m(a, b)$

   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 $m(ax_0 + by_0) > 0 \wedge m > 0 \implies ax_0 + by_0 > 0$

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

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

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

6. Demostrar: $d > 0 \wedge d|a \wedge d|b \implies \left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$

   Demostración:

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

$$\begin{aligned} (a, b) &= ax + by \qquad x, y \in \mathbb{Z} \\ &= dmx + dny \\ &= d(mx + ny) \end{aligned}$$

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

$$\frac{1}{d}(a, b) = mx + ny = \frac{a}{d}x + \frac{b}{d}y = \left(\frac{a}{d}, \frac{b}{d}\right)$$

   □

7. Demostrar: $(a, m) = (b, m) = 1 \implies (ab, m) = 1$

   Demostración:

   Como $(a, m) = ax + my = 1$ y $(b, m) = bu + mv = 1$

$$\begin{aligned} 1 &= (ax + my)(bu + mv) \\ &= (ax)(bu) + (ax)(mv) + (my)(bu) + (my)(mv) \\ &= ab(xu) + m(axv) + m(byu) + m(myv) \\ &= ab\underbrace{(xu)}_{\in\mathbb{Z}} + m\underbrace{(axv + byu + myv)}_{\in\mathbb{Z}} \\ &= (ab, m) \end{aligned}$$

   □

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

9. Demostrar: $c|ab \wedge (c, b) = 1 \implies c|a$

Demostración:

$(c,b) = 1 = cx + by, \quad x, y \in \mathbb{Z}$

$c|ab \implies ab = ck \implies k = \frac{a}{c}, \quad k \in \mathbb{Z}$ $\square$