Parcial 1.2 - Teoría de Números

Christian Mauricio Cardenas Baron
20251167009

Diego Andrés Capera Saenz
20251167019

Carlos Andres Giraldo Hernandez

Facultad de Ciencias Matemáticas y Naturales

Universidad Distrital Francisco José de Caldas

2025-10-16

1. Taller

1.1. Defina MCM de dos números y explique la importancia de la necesidad de las hipótesis.

Definición** (Mínimo Común Múltiplo)**:

Sean $a, b \in \mathbb{Z}$, ambos diferentes de cero, se tiene un múltiplo común c, si $a|c$ y $b|c$. El menor de los múltiplos comunes positivos recibe el nombre de *mínimo común múltiplo*, y se denota por $[a, b]$

Podemos identificar dos hipótesis principales:

i) Se toman a y b distintos de cero.

Si se toma $a = 0$. El único múltiplo de a es 0, por lo tanto limitaría los múltiplos comunes de a, b solamente a $\{0\}$, pero 0 no es positivo por lo tanto no cumpliría la segunda hipótesis, entonces no se tendría un mínimo común múltiplo.

«El razonamiento es análogo para $b = 0$»

ii) Se toma el menor de los múltiplos comunes **positivos**:

Esto se debe a que el conjunto de múltiplos comunes de a, b tiene una cantidad infinita de enteros positivos y negativos, Si no se limita a los positivos no abría un menor ya que el conjunto se extiende hasta $-\infty$

1.2. Ejemplifique y demuestre el método usado.

Ejemplo:

Para hallar $[15, 20]$. Se descomponen en factores primos 15 y 20 y para cada factor se toma el exponente máximo.

$$15 = 2^0 \cdot 3^1 \cdot 5^1$$
$$20 = 2^2 \cdot 3^0 \cdot 5^1$$
$$[15, 20] = 2^2 \cdot 3^1 \cdot 5^1 = 60$$

Demostración** (MCM por descomposición en factores primos)**:

Sea $a, b \in \mathbb{Z}$ ambos distintos de cero, por Teorema Fundamental de la Aritmética:

$|a| = \prod_{i=1}^{n} P_i^{\alpha_i} \quad |b| = \prod_{i=1}^{n} P_i^{\beta_i}$ Donde P_i son primos y $\alpha_i, \beta_i \in \mathbb{Z}_{\geq 0}$

Sea $m = \prod_{i=1}^{n} P_i^{\max(\alpha_i, \beta_i)}$.

Para que $[a, b] = m$, se debe cumplir:

1) $a|m$ y $b|m$

Fijamos un primo P_i.

- para a el exponente de P_i es α_i
- para b el exponente de P_i es β_i
- para m el exponente de P_i es $\max(\alpha_i, \beta_i)$

Como $\alpha_i \leq \max(\alpha_i, \beta_i)$, entonces $P_i^{\alpha_i} \mid P_i^{\max(\alpha_i,\beta_i)}$

Como $\beta_i \leq \max(\alpha_i, \beta_i)$, entonces $P_i^{\beta_i} \mid P_i^{\max(\alpha_i,\beta_i)}$.

Ademas esto se tiene para cada P_i, entonces:

$$\prod_{i=1}^{n} P_i^{\alpha_i} \mid \prod_{i=0}^{n} P_i^{\max(\alpha_i,\beta_i)} \wedge \prod_{i=1}^{n} P_i^{\beta_i} \mid \prod_{i=0}^{n} P_i^{\max(\alpha_i,\beta_i)}$$
$$a|m \qquad \wedge \qquad b|m$$

2) Para cualquier entero k si $a|k$ y $b|k$, entonces $m|k$

Sea $k \in \mathbb{Z}$ tal que $a|k$ y $b|k$, se toma la descomposición de k en los mismos factores primos que a, b

$$k = \prod_{i=1}^{n} \left(P_i^{\kappa_i}\right) \cdot Q$$

Con Q siendo otros posibles primos fuera de los factores de a, b

Como $a|k$, para cada i se tiene que $\alpha_i \leq \kappa_i$

Como $b|k$, para cada i se tiene que $\beta_i \leq \kappa_i$

Por lo tanto para cada i se tiene que $\max(\alpha_i, \beta_i) \leq \kappa_i$

Entonces tenemos que $P_i^{\max(\alpha_i,\beta_i)} | P_i^{\kappa_i}$

Por lo tanto

$$\prod_{i=1}^{n} P_i^{\max(\alpha_i,\beta_i)} \mid \prod_{i=1}^{n} P_i^{\kappa_i}$$
$$m \mid k$$

□

1.3. Extienda la definición de MCM a un conjunto de n números finito.

Definición:

Sean $a_1, a_2, ..., a_n$, todos diferentes de cero. Existe $b \in \mathbb{Z}$, que es múltiplo común de todos ellos si $b|a_1, b|a_2, ..., b|a_n$. El menor de los múltiplos comunes positivos recibe el nombre de *mínimo común múltiplo* y se denota por $[a_1, a_2, ..., a_n]$.

1.4. Realice una lista de 10 propiedades del MCM y demuéstralas.

1) Sean $a, b \in \mathbb{Z}$ no nulos. Entonces $[a, b] = [b, a] = [-a, b] = [a, -b] = [-a, -b]$

Demostración:

- $[a, b] = [b, a]$

  Sean $S_1 = \{m \in \mathbb{Z} : a|m\}$ y $S_2 = \{m \in \mathbb{Z} : b|m\}$, Tenemos que $\text{mul}(a, b) = S_1 \cap S_2$, pero también $\text{mul}(b, a) = S_2 \cap S_1$. Por lo tanto $\text{mul}(a, b) = \text{mul}(b, a)$, entonces sus mínimos son el mismo por lo tanto $[a, b] = [b, a]$

- $[a, b] = [-a, b] = [a, -b] = [-a, -b]$

  Por definición si $-a|m$, existe $l \in \mathbb{Z}$ tal que $m = (-a)l$, pero $m = a(-l)$, entonces $a|m$, por lo tanto conjuntos de múltiplos de a y $-a$ son iguales

  Por lo tanto $[a, b] = [-a, b]$, «analógicamente $[a, b] = [a, -b] = [-a, -b]$»

$\square$

2) Sean $a, b \in \mathbb{Z}$ no nulos. Entonces $m = [a, b]$ si y solo si
   1) $m > 0$
   2) $a|m$ y $b|m$
   3) Sea $k \in \mathbb{Z}$, si $a|k$ y $b|k$, entonces $m|k$

   Demostración:

- $\Longrightarrow$

  Supongamos $m = [a, b]$
  1) Por definición $m > 0$
  2) Por definición $a|m$ y $b|m$
  3) Sea $k \in \mathbb{Z}$ tal que $a|k$ y $b|k$.

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

$$k = mq + r, \quad 0 \leq r < m$$
$$k + m(-q) = r$$

     Si $r > 0$, como $a|k$ y $a|m$, entonces $a|r$, y como $b|k$ y $b|m$, entonces $b|r$. Ademas r seria divisor común de a y b, también $r < m$ lo que contradiría que m es el mínimo común múltiplo. Por lo tanto $r = 0$.

     Como $k = mq$, entonces $m|k$

- $\Longleftarrow$

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

  Sea $n \in \mathbb{Z}$ tal que $a|n$ y $a|n$, por hipótesis $m|n$, por lo tanto $m \leq n$

  Suponga otro m' que cumpla las propiedades, entonces $m|m' \Longrightarrow m \leq m'$, pero también $m'|m \Longrightarrow m' \leq m$, por lo tanto $m = m'$.

  Concluyendo $m = [a, b]$

$\square$

3) Sean $a_1, a_2, ..., a_n \in \mathbb{Z}$ no nulos. Entonces $m = [a_1, a_2, ..., a_n]$ si y solo si:
   1) $m > 0$
   2) $a_1|m, a_2|m, ..., a_n|m$

3) Sea $k \in \mathbb{Z}$, tal que $a_1|k, a_2|k, ..., a_n|k$, entonces $m|k$

Demostración:

- $\Longrightarrow$

  Suponga $m = [a_1, a_2, ..., a_n]$

  1) Por definición $m > 0$

  2) Por definición $a_i|m$ para $i = 1, 2, ..., n$

  3) Sea $k \in \mathbb{Z}$ tal que $a_i|k$ para $i = 1, 2, ..., n$

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

  $$k = mq + r, \quad 0 \leq r < m$$
  $$k + m(-q) = r$$

  Si $r > 0$, como $a_i|k$ y $a_i|m(-q)$ para $i = 1, 2, ..., n$, entonces $a|r$. Como $r < m$ se contradiría que m es el menor múltiplo común de a_i. Por lo tanto $r = 0$.

  Como $k = mq$, entonces $m|k$

- $\Longleftarrow$

  Suponga

  1) $m > 0$

  2) $a_i|m$ para $i = 1, 2, ..., n$

  3) Sea $k \in \mathbb{Z}$ tal que $a_i|k$ para $i = 1, 2, ..., n$, entonces $m|k$

  Como $m|k$, entonces $m \leq k$

  Sea m' que cumpla todas las condiciones anteriores, por *(3)* se tiene $m|m' \Longrightarrow m \leq m'$, pero también por *(3)* $m'|m \Longrightarrow m' \leq m$, por lo tanto $m = m'$

  Concluyendo $m = [a_1, a_2, ..., a_n]$

□

4) Sean $a_1, a_2, ..., a_n \in \mathbb{Z}$ todos distintos de cero, con $n > 2$. Entonces $[a_1, a_2, ..., a_n] = [[a_1, a_2, ..., a_{n-1}], a_n]$

Demostración:

Sea $L = [a_1, a_2, ..., a_{n-1}, a_n], \quad M = [a_1, a_2, ..., a_{n-1}], \quad R = [M, a_n]$

- Por definición M es múltiplo de $a_1, a_2, ..., a_{n-1}$. Como $R = [M, a_n]$, entones R es múltiplo de M, y también R es múltiplo de a_n, por lo tanto R es múltiplo de $a_1, a_2, ..., a_n$. Como $L = [a_1, a_2, ..., a_n]$, entonces $L|R$
- Por definición L es múltiplo de todos los a_i, en particular de $a_1, a_2, ..., a_{n-1}$, entonces L es múltiplo de M. También L es múltiplo de a_n,

por lo tanto L es múltiplo común de M y a_n. Como $R = [M, a_n]$, entonces $R|L$

Como $L|R$ y $R|L$, entonces $L = R$ □

5) Sean $a, b \in \mathbb{Z}$ no nulos. Entonces $[a, b] \cdot (a, b) = |ab|$

Demostración:

Sean las factorizaciones primas de a, b

$$|a| = \prod_{i=1}^{n} P_i^{\alpha_i} \qquad |b| = \prod_{i=1}^{n} P_i^{\beta_i}$$

Donde cada P_I es un numero primo distinto, y cada $\alpha_i, \beta_i \geq 0$.

Sabemos que $(a, b) = \prod_{i=1}^{n} P_i^{\min(\alpha_i, \beta_i)}$

También que $[a, b] = \prod_{i=1}^{n} P_i^{\max(\alpha_i, \beta_i)}$

Por lo tanto

$$(a, b) \cdot [a, b] = \prod_{i=1}^{n} P_i^{\min(\alpha_i, \beta_i)} \cdot \prod_{i=1}^{n} P_i^{\max(\alpha_i, \beta_i)} = \prod_{i=1}^{n} P_i^{\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_I)}$$

Ahora como $\alpha_i, \beta_i \geq 0$, entonces $\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$

$$\prod_{i=1}^{n} P_i^{\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_I)} = \prod_{i=1}^{n} P_i^{\alpha_i + \beta_I} = \prod_{i=1}^{n} P_i^{\alpha_i} \cdot \prod_{i=1}^{n} P_i^{\beta_I} = |a| \cdot |b| = |ab|$$

Por lo tanto $(a, b) \cdot [a, b] = |ab|$ □

6) Sean $a, b \in \mathbb{Z}$ no nulos. Entonces $[a, b] = |ab| \Longleftrightarrow (a, b) = 1$

Demostración:

- $\Longrightarrow$ Supongamos $[a, b] = |ab|$, como $[a, b] \cdot (a, b) = |ab|$, entonces $(a, b) = 1$
- $\Longleftarrow$ Supongamos $(a, b) = 1$, como $[a, b] \cdot (a, b) = |ab|$, entonces $[a, b] = |a, b|$

□

7) Sean $a, b \in \mathbb{Z}$ no nulos. Entonces $[a, b] = \frac{|ab|}{(a,b)}$

Demostración:

Sea $m = \frac{|ab|}{(a,b)}$

- Como $|ab| > 0$ y $(a, b) > 0$, entonces $m > 0$
- Sean $x, y \in \mathbb{Z}$ tal que $(x, y) = 1$

  Sea $d = (a, b)$, entonces $a = dx$ y $b = dy$

$$m = \frac{|ab|}{d} = \frac{|a||dy|}{d} = |a||y| = a(\pm y)$$

Por lo tanto $a|m$ «analógicamente $b|m$»

- Sea $k \in \mathbb{Z}$ tal que $a|k$ y $b|k$, existen $r, s \in \mathbb{Z}$ tal que $k = ar = bs \Longrightarrow (dx)r = (dy)s \Longrightarrow xr = ys$

  Ahora $y|xr$ y como $(x, y) = 1$, entonces $y|r$, existe $u \in \mathbb{Z}$ tal que $r = yu$

  Remplazando $k = ar = a(yu) = (ay)u = \pm mu$, por lo tanto $m|n$

$\square$

8) Sean $a, b \in \mathbb{Z}$ no nulos. Entonces $a|b \Longleftrightarrow [a, b] = |b|$

Demostración:

- $\Longrightarrow$

  Suponga $a|b$, entonces $(a, b) = |a|$, como $[a, b] \cdot (a, b) = |ab|$ remplazando

$$[a, b] \cdot |a| = |ab| \Longrightarrow [a, b] = \frac{|ab|}{|a|} \Longrightarrow [a, b] = |b|$$

- $\Longleftarrow$

  Suponga $[a, b] = |b|$, como $[a, b] \cdot (a, b) = |ab|$

$$|b| \cdot (a, b) = |ab| \Longrightarrow (a, b) = \frac{|ab|}{|b|} \Longrightarrow (a, b) = |a|$$

  Por lo tanto $|a| \mid b$, entonces $a|b$

$\square$

9) Sea $k \in \mathbb{Z}$ con $k > 0$. Entonces $[ma, mb] = m[a, b]$

Demostración:

Como $[a, b] = \frac{|ab|}{(a,b)}$, entonces

$$[ma, mb] = \frac{|ma \cdot mb|}{(ma, mb)} = \frac{|m^2 ab|}{m(a, b)} = \frac{m^2|ab|}{m(a, b)} = m\frac{|ab|}{(a, b)} = m[a, b]$$

$\square$

10) Sea $k \in \mathbb{Z}$ con $k > 0$. Entonces $\left[\frac{a}{k}, \frac{b}{k}\right] = \frac{[a,b]}{k}$

Demostración:

Como $[a, b] = \frac{|ab|}{(a,b)}$, entonces

$$\left[\frac{a}{k}, \frac{b}{k}\right] = \frac{|\frac{a}{k} \cdot \frac{b}{k}|}{\left(\frac{a}{k}, \frac{b}{k}\right)} = \frac{|\frac{ab}{k^2}|}{\frac{(a,b)}{k}} = \frac{\frac{|ab|}{k^2}}{\frac{(a,b)}{k}} = \frac{k|ab|}{k^2(a, b)} = \frac{1}{k} \cdot \frac{|ab|}{(a, b)} = \frac{1}{k} \cdot [a, b] = \frac{[a, b]}{k}$$

$\square$