Mínimo Común Múltiplo

Ana Ofelia Negrete Fernández

4 de agosto 2021

1. Introducción

Definiremos al **mínimo común múltiplo** de dos enteros a, b como el menor de los múltiplos comunes de a y b.

Ejemplificando, sean $a = 6$, $b = 8$. Obviamente, $6 \cdot 8 = 48$ es un múltiplo común para 6 y 8, pero no es el mínimo. Mientras que 24 sí lo es. El algoritmo para encontrar este número ya lo conocemos. En este caso:

8	6	2
4	3	2
2	3	2
1	3	3
	1	

Pensando en escribir esto con más formalidad, $6\mathbb{Z}$ tendría a todos los múltiplos de 6:

$$\{6, 12, 18, 24, 30, 36, 42, 48, \ldots\}.$$

A su vez, $8\mathbb{Z}$ serían los múltiplos de 8,

$$\{8, 16, 24, 32, 40, 48, \ldots\}.$$

De modo que al tomar la interseción $6\mathbb{Z} \cap 8\mathbb{Z}$, obtendríamos todos los múltiplos comunes de 8 y 6, de los cuales, el menor de ellos es el que nos interesaría; y que siempre existe; nos lo asegura el principio del buen orden. Más aún observamos que todos los múltiplos comunes de 6 y 8 son múltiplos de 24 (que era el mínimo de ellos). De tal suerte que $6\mathbb{Z} \cap 8\mathbb{Z} = 24\mathbb{Z}$.

2. Mínimo Común Múltiplo

En general sucederá que, para a y b enteros, todos los múltiplos comunes de a y b serán múltiplos del mínimo común múltiplo, llamémosle m; y denotémosle por $[a, b]$. Con ello tendremos la siguiente proposición, cuya demostración es inmediata y se deja como ejercicio.

Proposición 1. Si $a \neq 0$ o $b \neq 0$, $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, y $m \geq 0$, entonces

- $m > 0$,
- $a \mid m$ y $b \mid m$,
- Si $a \mid n$ y $b \mid n$, entonces $m \mid n$.

Para demostrar otra propiedad del MCM, primero hay que demostrar que:

Proposición 2. Sean $a, b, c \in \mathbb{Z}^+ \cup \{0\}$. Se cumple la igualdad

$$a\mathbb{Z}(b\mathbb{Z} \cap c\mathbb{Z}) = ab\mathbb{Z} \cap ac\mathbb{Z}.$$

Dem.- Primero notamos que $ab\mathbb{Z} = a\mathbb{Z}b\mathbb{Z}$, ya que cualquier $q \in ab\mathbb{Z}$ es de la forma $q = (ab)(z) = (az)(b \cdot 1)$. De este modo, $q \in a\mathbb{Z}b\mathbb{Z}$. Lo que demuestra $ab\mathbb{Z} \subseteq a\mathbb{Z}b\mathbb{Z}$. Y tomando $q \in a\mathbb{Z}b\mathbb{Z}$, tendríamos $q = az_1bz_2$, para algunos $z_1, z_2 \in \mathbb{Z}$. Luego, $az_1bz_2 = (ab)(z_1z_2) = abz$. De donde $q \in ab\mathbb{Z}$, de donde se deslinda $a\mathbb{Z}b\mathbb{Z} \subseteq ab\mathbb{Z}$.

De este modo, lo que nos piden demostrar es en realidad

$$a\mathbb{Z}(b\mathbb{Z} \cap c\mathbb{Z}) = a\mathbb{Z}b\mathbb{Z} \cap a\mathbb{Z}c\mathbb{Z}.$$

Sea $x \in a\mathbb{Z}(b\mathbb{Z} \cap c\mathbb{Z})$. Entonces x se puede escribir de dos maneras: $x = az_1bz_2$ o $x = az_1cz_3$. Claramente $az_1bz_2 \in a\mathbb{Z}b\mathbb{Z}$ y $az_1cz_2 \in a\mathbb{Z}c\mathbb{Z}$. Así, $x \in a\mathbb{Z}b\mathbb{Z} \cap a\mathbb{Z}c\mathbb{Z}$. Más aún, $x \in ab\mathbb{Z} \cap ac\mathbb{Z}$.

Ahora tomemos $x \in a\mathbb{Z}b\mathbb{Z} \cap a\mathbb{Z}c\mathbb{Z}$. De que $x \in a\mathbb{Z}b\mathbb{Z}$, sabemos que $x = az_1bz_2$, con $z_1, z_2 \in \mathbb{Z}$. De que $x \in a\mathbb{Z}c\mathbb{Z}$, se tiene que $x = az_1cz_3$, $z_3 \in \mathbb{Z}$. Por lo tanto, $x \in b\mathbb{Z} \cap c\mathbb{Z}$. Como $b\mathbb{Z} \cap c\mathbb{Z}$ es un ideal, existe $m \in \mathbb{Z}$ tal que $b\mathbb{Z} \cap c\mathbb{Z} = m\mathbb{Z}$, con $x = az_1mz_4 = a(z_1mz_4) = az$. Por lo que $x \in a\mathbb{Z}(b\mathbb{Z} \cap c\mathbb{Z})$.

□

Y ahora mostraremos que el MCM saca constantes.

Teorema 1. Si $k > 0$ y $k, b, c \in \mathbb{Z}$, se cumple: $[kb, kc] = k[b, c]$.

Dem.- Por defnción de mínimo común múltiplo tenemos que $[kb, kc]\mathbb{Z} = kb\mathbb{Z} \cap kc\mathbb{Z}$. Usando el lema, $kb\mathbb{Z} \cap kc\mathbb{Z} = k\mathbb{Z}(b\mathbb{Z} \cap c\mathbb{Z})$. Pero $b\mathbb{Z} \cap c\mathbb{Z} = [b, c]$, por definición de mínimo común múltiplo. Así, $k\mathbb{Z}(b\mathbb{Z} \cap c\mathbb{Z}) = k\mathbb{Z}([b, c])$ Finalmente, de la conmutatividad de la multiplicación en los enteros se tiene $k\mathbb{Z}([b, c]) = k\Big([b, c]\mathbb{Z}\Big)$.

□

Lema 1. Para $a, b \in \mathbb{Z}$ se cumple: $[a, b] = [-a, b] = [a, -b] = [-a, -b]$.

Dem.- Si a, b son distintos de cero, el mínimo común múltiplo $[a, b]$ es un entero positivo m, tal que $[a, b] = m$. De la proposición 1, sabemos que $a \mid m$ y $b \mid m$.

Esto es, existe $x \in \mathbb{Z}$ tal que $ax = m$. Que implica $(-a)(-x) = m$. Por lo que $-a \mid m$. Así, $[-a, b] = m$. Y por un argumento análogo, $[a, -b] = m$. Por último, ya que $a \mid m$ y $b \mid m$, tenemos que $ax = by = m$. Lo que implica $(-a)(-x) = (-b)(-y) = m = [-a, -b]$.

□

Notemos que si $b \neq 0$, y $a \mid b$, existe una **única** $c \in \mathbb{Z}$ tal que $ac = b$. Esto es una consecuencia de la ley de cancelación. Primero, $b \neq 0$ implica $a \neq 0$. Si existiera $d \in \mathbb{Z}$ tal que $ad = b$, sucedería $ad = ac$, lo que implica $d = c$.

Sólo si a divide a b y b es distinto de cero, denotaremos por $c = \frac{b}{a}$ al único entero x con la propiedad de que $ax = b$.

Ya mencionamos que para $a, b \in \mathbb{Z}$, multiplicar ab es obviamente múltiplo de a y b, pero no es siempre el mínimo. Lo que sí siempre sucederá es que ab se puede obtener multiplicando el MCM por el MCD, como lo establece el siguiente teorema:

Teorema 2. Si $a, b \in \mathbb{Z}$, $ab = (a, b)[a, b]$.

Dem.- El caso de $a = 0$, $b = 0$ se cumple evidentemente. Supongamos entonces $a \neq 0$ y $b \neq 0$. Por la observación previa al teorema, podemos tomar únicamente el caso $a > 0$ y $b > 0$; ya sabiendo qué pasa aquí, se deducirá lo que ocurre con los demás casos.

Luego, por la proposición 1, tomando $m = [a, b]$ tenemos que $a \mid m$ y $b \mid m$. Ya que a divide a m, existe $x \in \mathbb{Z}$ tal que $ax = m$, lo que implica, multiplicando por b, $abx = bm$. Es decir, $ab \mid b[a, b]$.

Más aún, sabemos que el mínimo común múltiplo divide a todos los múltiplos comunes de a y b, y ab es uno de ellos. De este modo $\frac{ab}{[a,b]} \mid b$.

Y de que $b \mid m$, podemos hacer un razonamiento análogo para deducir que $\frac{ab}{[a,b]} \mid a$.

Ya teniendo $\frac{ab}{[a,b]} \mid b$ y $\frac{ab}{[a,b]} \mid a$, concluimos que $\frac{ab}{[a,b]} \mid (a,b)$. Esto es porque (a,b) el máximo común divisor, es una combinación lineal de a y b y una propiedad de la divisibilidad nos decía: "Si $m,p,q \in \mathbb{Z}$, $m \mid p$ y $m \mid q$, entonces $m \mid \alpha s + \beta q \ \ \forall \alpha, \beta \in \mathbb{Z}$."

Por la misma propiedad de divisibilidad, si $\frac{ab}{[a,b]} \mid (a,b)$, entonces $\frac{ab}{[a,b]} \mid (a,b)[a,b]$. Lo que implica $(a,b) \mid \frac{ab}{[a,b]} \cdot y$. Nuevamente por la propiedad, $(a,b) \mid \left(\frac{ab}{[a,b]}\right) \cdot \left(y\right) \cdot \left(\frac{[a,b]}{y}\right)$. Es decir $(a,b) \mid ab$. Consecuentemente, $(a,b)[a,b]t = ab$, y por ende $ab \mid (a,b)[a,b]$, de la definición de divisibilidad y usando nuevamente la propiedad. De aquí concluimos que $(a,b)[a,b] \in ab\mathbb{Z}$.

Se demostró en la entrada de blog anterior que $(a,b) \mid a$ y $(a,b) \mid b$. Es decir, $(a,b)k = a$ y $(a,b)l = b$, para algunos $k,l \in \mathbb{Z}$. De donde $(a,b)k(a,b)l = ab$. Luego, $\frac{ab}{(a,b)} \in \mathbb{Z}$ implica que podemos dividir la anterior ecuación entre (a,b), obteniendo $al = bk = \frac{ab}{(a,b)}$.

Como se ve, $\frac{ab}{(a,b)}$, es múltiplo tanto de a como de b, por lo que también es múltiplo de $[a,b]$; así, $\frac{ab}{(a,b)} = w[a,b]$ para alguna $w \in \mathbb{Z}$ tal que $w > 0$. Igualdad que podemos multiplicar por (a,b). De modo que $ab = w[a,b](a,b)$.

Ya que $[a,b](a,b) \in ab\mathbb{Z}$, $ab = wabz$, lo que implica $wz = 1$, y de ello sabemos que w y z también son 1, pues los únicos enteros que tienen inverso multiplicativo son 1 y -1, pero elegimos $w > 0$, lo que descarta $w = z = -1$.

Se concluye $w = 1$, y así $ab = [a,b](a,b)$, como queríamos.

□

Ejemplo. El mínimo común múltiplo de 6 y 8 es $[6,8] = 24$. El máximo común divisor de 6 y 8 es $(6,8) = 2$. De este modo, $[6,8](6,8) = (2)(24) = 48 = (6)(8)$.

El teorema 2 afirma que esto pasa para cada par de enteros que elijamos. Podríamos estar todo el día jugando con parejas de enteros m,n, fueran estos ambos positivos, ambos negativos, uno y uno, números muy grandes o chicos o combinados, y así nos daríamos cuenta de que multiplicar m por n da lo mismo que calcular el máximo común divisor (m,n), luego el mínimo común múltiplo $[m,n]$ y multiplicar $(m,n)[m,n]$. Si se te ocurre una aplicación interesante para este resultado, te invito a que me lo cuentes.

Y por supuesto que nos interesaría saber si podemos calcular el mínimo común múltiplo para n enteros, lo que siempre es posible pues éste número siempre existe, aunque sean muchos los enteros involucrados, y es lo que mostraremos a continuación.

Teorema 3. Sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ tales que $a_n \neq 0 \ \ \forall n$. El máximo común divisor de n números es

$$\Big[a_1, a_2, \ldots, a_n\Big] = \Big[[a_1, a_2, \ldots, a_{n-1}], a_n\Big].$$

Dem.- Haremos una prueba por inducción, donde el caso base consiste en mostrar que

$$\Big[a_1, a_2, a_3\Big] = \Big[[a_1, a_2], a_3\Big].$$

$\Big[[a_1, a_2], a_3\Big] = [a_1, a_2]\mathbb{Z} \cap a_3\mathbb{Z} = (a_1\mathbb{Z} \cap a_2\mathbb{Z}) \cap a_3\mathbb{Z} = a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap a_3\mathbb{Z}$, por definición de mínimo común múltiplo y la asociatividad de la intersección de conjuntos.

Como la intersección de ideales es un ideal, existe $m \in \mathbb{Z}$ tal que

$$m\mathbb{Z} = a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap a_3\mathbb{Z} = [a_1, a_2, a_3].$$

Suponemos, por hipótesis de inducción, que $[a_1, a_2, \ldots, a_{n-1}] = \Big[[a_1, a_2, \ldots, a_{n-2}], a_{n-1}\Big]$, y queremos demostrar $[a_1, a_2, \ldots, a_n] = \Big[[a_1, a_2, \ldots, a_{n-1}], a_n\Big]$.

Ya que, por hipótesis de inducción existe $q \in \mathbb{Z}$ tal que $q\mathbb{Z} = a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \ldots \cap a_{n-1}\mathbb{Z}$,

$$\begin{aligned}\Big[[a_1, a_2, \ldots, a_{n-1}], a_n\Big] &= q\mathbb{Z} \cap a_n\mathbb{Z} \\ &= (a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \ldots \cap a_{n-1}\mathbb{Z}) \cap a_n\mathbb{Z} \\ &= a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \ldots \cap a_{n-1}\mathbb{Z} \cap a_n\mathbb{Z}.\end{aligned}$$

La última igualdad formalmente también se demuestra por inducción, usando el hecho de que la intersección de conjuntos es un conjunto y reduciendo todo al caso base para dos conjuntos.

Dado que la intersección de ideales es un ideal, $\exists w \in \mathbb{Z}$ tal que

$$w\mathbb{Z} = q\mathbb{Z} \cap a_n\mathbb{Z} = [a_1, a_2, \ldots, a_n].$$

Por lo tanto,

$$w\mathbb{Z} = [a_1, a_2, \ldots, a_n] = \Big[[a_1, a_2, \ldots, a_{n-1}], a_n\Big].$$

□

A veces se dice que la definición de $[a_1, a_2, \ldots, a_n]$ es $\Big[[a_1, a_2, \ldots, a_{n-1}], a_n\Big]$ y se omite una demostración.

3. Más propiedades para el Máximo Común Divisor

Para finalizar este texto, demostraremos dos resultados sobre máximo común divisor, además de los que ya teníamos, y que se parecen a lo que ya hemos hecho hoy.

Primero una proposición que nos servirá para una de las pruebas.

Proposición 3. Sean $a, b, c \in \mathbb{Z}$.Se cumple la igualdad: $a\mathbb{Z}(b\mathbb{Z} + c\mathbb{Z}) = a\mathbb{Z}b\mathbb{Z} + a\mathbb{Z}c\mathbb{Z}$.

Dem.- Para verificar que $a\mathbb{Z}(b\mathbb{Z} + c\mathbb{Z}) \subseteq a\mathbb{Z}b\mathbb{Z} + a\mathbb{Z}c\mathbb{Z}$, tomemos $x \in a\mathbb{Z}(b\mathbb{Z} + c\mathbb{Z})$. Entonces $x = az_1(bz_2 + cz_3)$, para algunos $z_1, z_2, z_3 \in \mathbb{Z}$. Y por la distributividad y asociatividad en $\mathbb{Z}$ se tiene que

$$x = (az_1)(bz_2) + (az_1)(cz_3) \in a\mathbb{Z}b\mathbb{Z} + a\mathbb{Z}c\mathbb{Z}.$$

La contención $a\mathbb{Z}b\mathbb{Z} + a\mathbb{Z}c\mathbb{Z} \subseteq a\mathbb{Z}(b\mathbb{Z} + c\mathbb{Z})$ es igualmente fácil. Toda la igualdad se pudo haber demostrado directamente, pues, cada uno de los pasos del párrafo anterior es un si y sólo sí.

□

Y ahora, veremos que el MCD saca constantes. O lo que es mismo, da igual calcular un máximo común divisor de (b, c) y luego multiplicarlo por una constante, que multiplicar primero b y c por una constante antes de calcularle a eso el máximo común divisor.

Teorema 4. Si $k, b, c \in \mathbb{Z}$ y $k > 0$, entonces $(kb, kc) = k(b, c)$.

Dem.- Tenemos que

$$\begin{aligned}k(b,c)\mathbb{Z} &= k\mathbb{Z}((b,c)\mathbb{Z}) && \text{(se demostró en la proposición 2)} \\ &= k\mathbb{Z}(b\mathbb{Z} + c\mathbb{Z}) && \text{(definición de } (b,c)) \\ &= k\mathbb{Z}b\mathbb{Z} + k\mathbb{Z}c\mathbb{Z} && \text{(proposición 3)} \\ &= kb\mathbb{Z} + kc\mathbb{Z} && \text{(conmutatividad y asociatividad en } \mathbb{Z}) \\ &= (kb, kc)\mathbb{Z}. && \text{(definición de } (kb,kc))\end{aligned}$$

De este modo, $k(b, c) \mid (kb, kc)$ y $(kb, kc) \mid k(b, c)$. Ya que ambos $k(b, c)$ y (kb, kc) son no negativos, se garantiza la igualdad $k(b, c) = (kb, kc)$.

□

Teorema 5. Sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ tales que $a_n \neq 0$ para toda $n \in \mathbb{N}$. El máximo común divisor de n números es

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n).$$

Dem.- Haremos la prueba por inducción, donde el caso base es $(a_1, a_2, a_3) = ((a_1, a_2), a_3)$. No hay tanto que demostrar, pues esta es la definición de máximo común divisor para tres números, y aquí la razón de ello:

Sea $(a_1, a_2) = m_1$.

$$\begin{aligned} ((a_1, a_2), a_3) &= (a_1, a_2)\mathbb{Z} + a_3\mathbb{Z} \\ &= (a_1\mathbb{Z} + a_2\mathbb{Z}) + a_3\mathbb{Z} \\ &= a_1\mathbb{Z} + a_2\mathbb{Z} + a_3\mathbb{Z} \\ &= (a_1, a_2, a_3). \end{aligned}$$

Notamos que ya que el máximo común divisor para dos números está definido, entonces el máximo común divisor de tres números está definido, pues existirá el generado de (a_1, a_2) y a_3:

$$(a_1, a_2)\mathbb{Z} + a_3\mathbb{Z} = m_1\mathbb{Z} + a_3\mathbb{Z} = \langle\{m_1, a_3\}\rangle = m_2\mathbb{Z},$$

con $m_2 \in \mathbb{Z}$, $m_2 > 0$. Como la suma en $\mathbb{Z}$ es asociativa, $((a_1, a_2), a_3) = (a_1, (a_2, a_3)) = (a_1, a_2, a_3)$.

Además sucederá que $0 \leq m_2 \leq m_1$, pues m_2 divide a m_1.

Ya que el máximo común divisor para tres números está definido, también lo está el máximo común divisor para n números, y la prueba de esto formalmente se hace por inducción, y reduciendo el problema al caso base de una suma de dos términos.

Supongamos ahora por hipótesis de inducción, $(a_1, a_2, \ldots, a_{n-1}) = ((a_1, a_2, \ldots, a_{n-2}), a_{n-1})$.

Queremos demostrar que $(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$.

La hipótesis nos dice que existe un entero m_{n-1} tal que $m_{n-1}\mathbb{Z} = \langle\{a_1, a_2, \ldots, a_{n-1}\}\rangle$, y de este modo estará también definido el máximo común divisor para n números, simplemente sumando:

$$((a_1, a_2, \ldots, a_{n-1}), a_n) = m_n\mathbb{Z} = m_{n-1}\mathbb{Z} + a_n\mathbb{Z}.$$

Más aún, de la asociatividad en $\mathbb{Z}$ se tiene que

$$\begin{aligned} m_{n-1}\mathbb{Z} + a_n\mathbb{Z} &= (a_1\mathbb{Z} + a_2\mathbb{Z} + a_{n-1}\mathbb{Z}) + a_n\mathbb{Z} \\ &= a_1\mathbb{Z} + a_2\mathbb{Z} + a_{n-1}\mathbb{Z} + a_n\mathbb{Z} \\ &= (a_1, a_2, \ldots, a_n), \end{aligned}$$

por lo que $(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$.

Además, $0 \leq m_n \leq m_{n-1} \leq \ldots \leq m_1$, pues $m_n \mid m_{n-1}$, $m_{n-1} \mid m_{n-2}, \ldots \ m_2 \mid m_1$, por cómo se fueron construyendo los $m_i\mathbb{Z}$.

□

4. Ejercicios

- Demuestra que, para $a, b \in \mathbb{Z}$ se cumple: $(a, b) = (-a, b) = (a, -b) = (-a, -b)$.
- Demuestra que, en $\mathbb{Z}$, el mínimo común múltiplo y el máximo común divisor son únicos.