Olimpiada Básica de Matemáticas en Guanajuato
@OBMGuanajuato | 10 de septiembre del 2022

Máximo común divisor y Mínimo común múltiplo

Emilio Toscano Oneto

1 Máximo común divisor

Recordemos rápidamente que para dos enteros a y b, cuando escribimos $a \mid b$, esto hace referencia a que a divide a b, y es equivalente a otras expresiones como b es múltiplo de a, a es divisor de b, entre otros. Similarmente, se tiene la negación $a \nmid b$, la cuál significa que a no divide a b.

Cuando escribimos $|a|$ para algún entero a, nos referimos al valor absoluto, es decir, si a es tal que $a \geq 0$, entonces $|a| = a$, mientras que si $a < 0$, entonces $|a| = -a$, es decir, se puede pensar a $|a|$ como la versión positiva del entero a.

Definición 1.1. *Para una colección de enteros $a_1, a_2, ..., a_n$ distintos de 0, decimos que su máximo común divisor, denotado por $\text{mcd}(a_1, ..., a_n)$, es el mayor divisor que los enteros $a_1, ..., a_n$ tienen en común, es decir, $d = \text{mcd}(a_1, ..., a_n)$ si cumple que $d \mid a_1, ..., d \mid a_n$ y cualquier otro entero que satisface estas condiciones es menor o igual a d.*

Ejemplo 1.2. *Hallar el máximo común divisor de los enteros 24, 30 y 18.*

Empecemos listando los divisores de cada número.

- *Los divisores del 24 son:* $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24$.
- *Los divisores del 30 son:* $\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30$.
- *Los divisores del 18 son:* $\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18$.

De donde los divisores en común de los números son $\pm 1, \pm 2, \pm 3$ y ± 6, donde el más grande de todos ellos es 6.

Nota 1.3. *Se puede observar que listar todos los divisores de varios números es una tarea tediosa, sin embargo, más adelante veremos una forma más simple de calcular el máximo común divisor.*

Observación 1.4. *Siempre se cumple que $\text{mcd}(a_1, a_2, ..., a_n) = \text{mcd}(a_1, \text{mcd}(a_2, ..., a_n))$, por lo que a partir de aquí se trabajará con $n = 2$.*

Proposición 1.5. *Sean a y b enteros distintos de 0. Las siguientes afirmaciones se cumplen:*
(i) $\text{mcd}(a, b) = \text{mcd}(|a|, |b|)$.
(ii) $\text{mcd}(a, b) > 0$.
(iii) Si $a \mid b$, entonces $\text{mcd}(a, b) = |a|$.
(iv) Si $d = \text{mcd}(a, b)$, entonces $a = da'$ y $b = db'$ para ciertos enteros a' y b' que además satisfacen que $\text{mcd}(a', b') = 1$.

Demostración de Proposición 1.5 : La demostración de (i) queda como ejercicio moral para el lector.

(ii) Puesto que el 1 divide a cualquier entero, entonces $1 \mid a$ y $1 \mid b$, por lo que $\text{mcd}(a,b) \geq 1 > 0$.

(iii) Si $a \mid b$, entonces $b = ac$ para algún entero c, por lo que usando el numeral (i), se sigue que $\text{mcd}(a,b) = \text{mcd}(|a|,|ac|) = \text{mcd}(|a|,|a|\,|c|) = |a|$.

(iv) Si $d = \text{mcd}(a,b)$, entonces $d \mid a$ y $d \mid b$, por lo que existen enteros a' y b' tales que $a = da'$ y $b = db'$. Supongamos que $\text{mcd}(a',b') = n$; nuevamente se tiene que $a' = na''$ y $b' = nb''$ para ciertos enteros a'' y b'', más aún, se tiene que $a = dna''$ y $b = dnb''$, de donde $dn \geq d$ divide a ambos a y b, pero por definición de d la única manera de que esto sea posible es si $n = 1$.
■

De manera más general, cuando $\text{mcd}(a,b) = 1$, decimos que a y b son primos relativos, primos entre sí ó coprimos.

Ejemplo 1.6. *Los números* 18 *y* 35 *son coprimos, pues los divisores de* 35 *son* $\pm 1, \pm 5, \pm 7$ *y* ± 35 *y anteriormente vimos los divisores de* 18*, de donde únicamente comparten a* ± 1 *como divisor, por ende* $\text{mcd}(18,35) = 1$.

Es claro ver que cualquier par de números primos p y q son coprimos y que para cualquier entero k que no es múltiplo de p, k y p son coprimos.

Lema 1.7. *Sean a y b enteros distintos de* 0 *con* $b \nmid a$. *Si q y r son enteros tales que* $a = bq + r$*, entonces* $\text{mcd}(a,b) = \text{mcd}(b,r)$.

Demostración de Lema 1.7 : Si $d = \text{mcd}(a,b)$, entonces por la Proposición 1.5, se tiene que $a = da'$ y $b = db'$ para ciertos enteros a' y b', por lo tanto vemos que $r = a - bq = da' - db'q = d(a' - b'q)$ de donde $d \mid r$.

Por otro lado, sea $c = \text{mcd}(b,r)$, tenemos que $b = cb''$ y $r = cr'$, de donde $a = c(b''q + r')$, es decir, $c \mid a$. De esto último, se sigue que c divide a ambos a y b y así $c \leq d$, por definición de $\text{mcd}(a,b)$, recíprocamente, d divide a b y r, de donde $d \leq c$, luego $c \leq d \leq c$ implica que $c = d$, por lo tanto, $\text{mcd}(a,b) = \text{mcd}(b,r)$.
■

Este resultado, junto con el algoritmo de la división será de utilidad para mostrar el siguiente resultado el cuál es importante para poder calcular el máximo común divisor de dos números o más.

Teorema 1.8. ***(Algoritmo de Euclides.)*** *Sean a y b enteros distintos de* 0*. Entonces* $\text{mcd}(a,b)$ *es combinación lineal de a y b.*

Demostración de Teorema 1.8 : Supongamos que a y b son enteros positivos (el caso con negativos es completamente analogo), si $a \mid b$, entonces $\text{mcd}(a,b) = a$ y el resultado es claro. En caso contrario, utilizando el algoritmo de la división, existen enteros q_i y r_i para $i = 1, ..., n$ tales que

$$\begin{aligned}
a &= bq + r_1, & 0 < r_1 < b,\\
b &= r_1 q_1 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3, & 0 < r_3 < r_2,\\
&\vdots & \vdots\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1},\\
r_{n-1} &= r_n q_n
\end{aligned}$$

Por el Lema 1.7, sabemos que se cumple que

$$\text{mcd}(a,b) = \text{mcd}(b,r_1) = \text{mcd}(r_1,r_2) = \cdots = \text{mcd}(r_{n-1},r_n) = r_n.$$

Ahora, notemos que $r_1 = a+b(-q)$ es combinación lineal de a y b, y así de la segunda ecuación, se reescribe a r_2 como $r_2 = a(-q_1) + b(1+qq_1)$, este proceso se puede realizar repetidas veces hasta tener que r_n es combinación lineal de a y b lo que concluye la prueba.
■

Nota 1.9. *La justificación anterior de "este proceso se puede realizar varias veces", se puede formilizar con el método de inducción, sin embargo, no incluiremos este tema aquí.*

A partir de está demostración, se puede observar que se consigue un método más práctico de calcular el máximo común divisor de dos números e inversamente, de escribir al $\text{mcd}(a,b)$ como combinación lineal de a y b.

Ejemplo 1.10. *Calcula el máximo común divisor de* 36 *y* 60. *Por el algoritmo de la división, se observa que*

$$\begin{aligned} 60 &= 36 \times 1 + 24 \\ 36 &= 24 \times 1 + 12 \\ 24 &= 12 \times 2 \end{aligned}$$

Por lo que $\text{mcd}(36,60) = 12$.

Ejemplo 1.11. *Escribe a* 21 *y* 51 *como combinación lineal de su máximo común divisor. Primero veamos que*

$$\begin{aligned} 51 &= 21 \times 2 + 9 \\ 21 &= 9 \times 2 + 3 \\ 9 &= 3 \times 3 \end{aligned}$$

Por lo tanto, $\text{mcd}(21,51) = 3$, *y para escribirlo como combinación lineal de* 21 *y* 51, *despejamos desde la penúltima ecuación*

$$\begin{aligned} 3 &= 21 - 9 \times 2 \\ 9 &= 51 - 21 \times 2 \end{aligned}$$

De donde $3 = 21 - (51 - 21 \times 2) \times 2$, *es decir,* $3 = 21(5) + 51(-2)$.

Corolario 1.12. *Para a y b enteros distintos de* 0 *y* $d = \text{mcd}(a,b)$, *se cumple que un entero c es combinación lineal de a y b si y sólo si es múltiplo de d.*

Demostración de Corolario 1.12 : Si c es combinación lineal de a y b, entonces como $d \mid a$ y $d \mid b$, se sigue que $d \mid c$. Por otro lado, si $c = dc'$, por el Teorema 1.8, $d = ar + bs$ para ciertos enteros r y s, y así $dc' = arc' + bsc'$, es decir, $c = a(rc') + b(sc')$.
■

Ejemplo 1.13. *Determina si* 10 *y* 20 *son combinaciones lineales de* 12 *y* 28. *Se puede comprobar que* $\text{mcd}(12, 28) = 4$, *pero* $4 \nmid 10$, *y* 10 *no puede ser combinación lineal de* 12 *y* 28. *Por otro lado,* $4 \mid 20$ *y puesto que* $4 = 12(-2) + 28$, *entonces al multiplicar por* 5 *se sigue que* $20 = 12(-10) + 28(5)$.

Proposición 1.14. *Sean los enteros* a *y* b *con descomposición canónica* $a = \pm p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ *y* $b = \pm p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$, *es decir,* $p_1 < p_2 < ... < p_k$ *son primos y los números* n_i *y* m_i *son enteros no negativos para todo* $i = 1, ..., k$. *Sea* $d = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$ *como en la descomposición anterior, donde* r_i *es el mínimo entre* n_i *y* m_i *(escrito como* $\min\{n_i, m_i\}$*) para cada* i, *entonces* $d = \text{mcd}(a, b)$.

Demostración de Proposición 1.14 : Es claro que $d \mid a$ y $d \mid b$, y basta con demostrar que es el mayor que lo cumple. Sea c un entero tal que $c \mid a$ y $c \mid b$, entonces su descomposición canónica es de la forma $c = p_1^{s_1} p_2^{s_2} ... p_k^{s_k}$ tal que $s_i \leq n_i$ y $s_i \leq m_i$, para $i = 1, ..., k$. Puesto que $r_i = \min\{n_i, m_i\}$, entonces $s_i \leq r_i$ para cualquier i, y así $c \mid d$, por lo que $c \leq d$ y d es el máximo común divisor de a y b.
■

Ejemplo 1.15. *Calcula* $\text{mcd}(24, 54, 84)$. *Puesto que* $24 = 2^3 \times 3$, $54 = 2 \times 3^3$ *y* $84 = 2^2 \times 3 \times 7$, *entonces se tiene que* $\text{mcd}(24, 54, 84) = 2 \times 3 \times 7^0 = 6$.

2 Mínimo común múltiplo

Definición 2.1. *Sean* $a_1, a_2, ..., a_k$ *enteros distintos de* 0, *definimos al mínimo común múltiplo (denotado por* $\text{mcm}(a_1, a_2, ..., a_k)$*) como el menor entero que es múltiplo positivo de cada uno de ellos.*

Ejemplo 2.2. *Para* 9 *y* 12, *los primeros múltiplos de* 9 *son* $9, 18, 27, 36, 45$, *etc. Mientras que los primeros múltiplos de* 12 *son* $12, 24, 36, 48, 60$, *etc. De donde se observa que el primer número en coincidir es* 36, *por lo tanto,* $\text{mcm}(9, 12) = 36$.

Observación 2.3. *Analogamente al caso del máximo común divisor, se cumple* $\text{mcm}(a_1, a_2, ..., a_k) = \text{mcm}(a_1, \text{mcm}(a_2, ..., a_k))$, *por lo que basta demostrar los siguientes resultados para* 2 *enteros.*

Proposición 2.4. *Sean* a *y* b *enteros distintos de* 0, *entonces las siguientes afirmaciones se cumplen:*
(i) $\text{mcm}(a, b)$ *es divisor de cualquier múltiplo común de* a *y* b.
(ii) Si $a = \pm p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ *y* $b = \pm p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$ *con* p_i *primos distintos y* n_i *y* m_i *enteros no negativos, entonces* $\text{mcm}(a, b) = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$, *donde* $r_i = \max\{n_i, m_i\}$ *para cada* $i = 1, ..., k$ *(r_i es el máximo valor entre* n_i *y* m_i*).*

La demostración del numeral (i) de la Proposición 2.4 es inmediata de la definición de mcm y la del numeral (ii) queda como ejercicio moral para el lector, pues es muy similar a la del Corolario 1.12.

Teorema 2.5. *Sean* a *y* b *enteros distintos de* 0, *entonces* $\text{mcd}(a, b) \cdot \text{mcm}(a, b) = |ab|$.

Demostración de Teorema 2.5 : Notemos que la descomposición canónica de $|ab|$ esta dada por

$$|ab| = p_1^{n_1 + m_1} p_2^{n_2 + m_2} ... p_k^{n_k + m_k}$$

Donde $a = \pm p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ y $b = \pm p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$, con p_i primos distintos y $n_i, m_i \geq 0$ para todo $i = 1, ..., k$. De esta forma, para cada i, el valor $\min\{n_i, m_i\}$ es uno de los dos valores n_i o m_i, mientras que $\max\{n_i, m_i\}$ es el otro, y así por la Proposición 1.14 y 2.4

$$\text{mcd}(a, b) \cdot \text{mcm}(a, b) = p_1^{n_1+m_1} p_2^{n_2+m_2} ... p_k^{n_k+m_k}$$

De donde se concluye el resultado.
■

3 Ejercicios

La siguiente lista de ejercicios no lleva ningún orden particular de dificultad.

Ejercicio 3.1. *Sean a y b enteros distintos de 0 y $d = \text{mcd}(a, b)$. Demuestra que cualquier divisor común de a y b también es divisor de d.*

Ejercicio 3.2. *Sean a, b y c enteros tales que $a \mid bc$. Demuestra que si a y b son coprimos, entonces $a \mid c$.*

Ejercicio 3.3. *Prueba que $\text{mcd}(2^n - 1, 2^m - 1) = 2^d - 1$, donde $d = \text{mcd}(n, m)$.*

Ejercicio 3.4. *Calcula el máximo común divisor de $2^{12} - 1$ y $3^{12} - 1$.*

Ejercicio 3.5. *Si p es un número primo, demuestra que $\sqrt{p}$ no es un número racional (un racional es un número de la forma $\frac{a}{b}$ para a y b enteros con b distinto de 0).*

Ejercicio 3.6. *Demuestra que para a, b y n enteros, se cumple que $\text{mcd}(a, b) = \text{mcd}(a, b - an) = \text{mcd}(a - bn, b)$.*

Ejercicio 3.7. *Sean a, b y n enteros positivos, demuestra que $\text{mcd}(an, bn) = n \cdot \text{mcd}(a, b)$.*

Ejercicio 3.8. *Si a y b son coprimos. ¿Se cumple que a^2 y b^2 son coprimos?*

Ejercicio 3.9. *Demuestra que para a y b enteros coprimos,*

$$\text{mcd}(a + b, a^2 - ab + b^2) = 1 \text{ o } 3,$$

Ejercicio 3.10. *Sean a y b enteros coprimos tales que $ab = c^n$ para ciertos enteros c y n. Demuestra que existen enteros x y y tales que $a = x^n$ y $b = y^n$.*

Ejercicio 3.11. *Si a, b y c son enteros tales que $a \mid c$ y $b \mid c$, y $d = \text{mcd}(a, b)$, demuestra que $\frac{ab}{d}$ también divide a c.*

Ejercicio 3.12. *Si a y b son coprimos, demuestra que $\text{mcd}(a + b, a - b) = 1$ o 2.*

Ejercicio 3.13. *Si* $a = 2^n \times 15$, $b = 3^m \times 4$ *y* $\operatorname{mcm}(a,b) = 360$. *Calcula* $n+m$.

Ejercicio 3.14. *Demuestra que* $21n+4$ *y* $14n+3$ *son coprimos para cualquier entero positivo* n.

Ejercicio 3.15. *Calcula* $\operatorname{mcm}(2018!+1, 2019!)$ *(Recuerda que* $n! = n \times (n-1) \times ... \times 2 \times 1$*).*

Ejercicio 3.16. *Sean* a *y* b *enteros positivos y* $\operatorname{mcd}(a,b) = d$. *Demuestra que si* $\frac{a+1}{b} + \frac{b+1}{a}$ *es un entero, entonces* $d \leq \sqrt{a+b}$.

Ejercicio 3.17. *Demuestra que para* a, b *y* c *enteros, entonces* $\operatorname{mcd}(a,b,c)$ *es combinación lineal de* a, b *y* c.

Ejercicio 3.18. *Sean* a *y* b *enteros coprimos, entonces demuestra que* x *y* y *es solución a la ecuación* $ax + by = 0$ *si y sólo si* $x = -bt$ *y* $y = at$ *para* t *entero.*

Ejercicio 3.19. *Encuentra todas las soluciones enteras de la ecuación* $282x - 195y = 7$.

Ejercicio 3.20. *Demuestra que no hay soluciones enteras* a *y* b *para la ecuación* $18a + 42b = 5$.

Ejercicio 3.21. *Para* a, b *y* c *enteros, demuestra que*

$$\frac{(\operatorname{mcm}(a,b,c))^2}{\operatorname{mcm}(a,b)\operatorname{mcm}(b,c)\operatorname{mcm}(c,a)} = \frac{(\operatorname{mcd}(a,b,c))^2}{\operatorname{mcd}(a,b)\operatorname{mcd}(b,c)\operatorname{mcd}(c,a)}$$

Ejercicio 3.22. *Si* $\operatorname{mcd}(a,b,c) = 1$, *demuestra que* $\operatorname{mcd}(a+b+c, ab+bc+ac, abc) = 1$.

Ejercicio 3.23. *Sean* a, b *y* c *enteros impares, demuestra que*

$$\operatorname{mcd}\left(\frac{a+b}{2}, \frac{b+c}{2}, \frac{c+a}{2}\right) = \operatorname{mcd}(a,b,c).$$

Ejercicio 3.24. *Prueba que para* a *y* b *enteros, no es posible que* $a + b = \operatorname{mcm}(a,b)$.

Ejercicio 3.25. *Si para enteros positivos* a *y* b *se cumple que* $a + b = 2022$ *y* $\operatorname{mcm}(a,b) = 2018 \operatorname{mcd}(a,b)$. *Calcula* $\operatorname{mcm}(a,b)$.

Ejercicio 3.26. *Demuestra que no existen enteros* a, b *y* c *tales que* $\operatorname{mcm}(a,b) + \operatorname{mcm}(b,c) + \operatorname{mcm}(c,a) = \operatorname{mcm}(a,b,c)$.

Ejercicio 3.27. *Sean* a *y* b *enteros positivos tales que* $\operatorname{mcm}(a,b) = 88$ *y* $a^2 + b^2 = 2000$. *Calcula* $a + b$.

Ejercicio 3.28. *Sean* $M = \operatorname{mcm}(10, 11, ..., 29, 30)$ *y* $N = \operatorname{mcm}(M, 32, 33, ..., 39, 40)$. *Calcula* $\frac{N}{M}$.

Ejercicio 3.29. *Si para dos enteros positivos* a *y* b, *se cumple que* $\operatorname{mcm}(a,b) + \operatorname{mcd}(a,b) = p$ *para* p *un número primo, demuestra que* $\operatorname{mcd}(a,b) = 1$.

Ejercicio 3.30. *Encuentra todos los enteros positivos* a *y* b *que satisfacen la siguiente ecuación*

$$ab + 63 = 20 \operatorname{mcm}(a,b) + 12 \operatorname{mcd}(a,b).$$