34 Olimpiada Mexicana de MATEMÁTICAS Aguascalientes 2020

MCD y MCM

Daniela Maribel Trancoso Cervantes

1. Repaso de divisibilidad

El conjunto de los números naturales es $\mathbb{N} = \{1, 2, 3, \dots\}$ y el conjunto de los números enteros es $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$.
Decimos que un entero b es divisible por un entero a (diferente de cero), si existe un entero x tal que podamos escribir a b como $b = a \cdot x$. Que b sea divisible por a, se denotará por $a|b$, que b no es divisible por a, lo denotamos por $a \nmid b$. Si $a|b$, también se acostumbra a decir que a es divisor o factor de b, o que b es múltiplo de a.

2. Algoritmo de la división

Si tenemos dos enteros a y b, con $b \neq 0$, existen dos enteros q y r tales que $a = bq + r$ y $0 \leq r < b$.

Al número a se le llama dividendo.

Al número b se le llama divisor.

Al número q se le llama cociente.

Al número r se le llama residuo.

En el caso particular que a y b sean enteros positivos, se trata de hallar el número de veces que el dividendo contiene al divisor. Este número se llama cociente, y lo que queda se llama residuo.

Ejemplo: Si queremos encontrar el resultado de dividir 34 entre 5 tenemos:

$$34 = 5 \cdot 6 + 4,$$

es decir, que el cociente es 6 y el residuo 4. Se puede observar que el residuo 4 es mayor que 0 y menor que 5 que es el divisor.

Ejemplo: Para hallar el resultado de dividir 23 entre 7 tenemos:

$$23 = 7 \cdot 3 + 2,$$

lo que quiere decir que el cociente es 3 y el residuo es 2.

Cuando el residuo es cero, se dice que la división es exacta y en este caso se cumple que el dividendo es igual al divisor por el cociente, es decir, $a = bq$. Con lo cual podemos decir también que b es divisor o factor de a ($b|a$).

3. Máximo común divisor

Decimos que d es el **máximo común divisor (MCD)** de dos números naturales a y b, y se escribe $d = mcd(a, b)$, si se cumplen las siguientes dos condiciones:

1. $d|a$ y $d|b$, es decir, d es un divisor común de a y de b.
2. c es tal que $c|a$ y $c|b$, entonces $c \leq d$; es decir, no existe un divisor común de a y b que sea mayor a d.

En otras palabras, el máximo común divisor de a y b es el mayor entero que divide a ambos números. Otra notación utilizada para expresar el máximo común divisor de dos números a y b es (a, b).

Algunas propiedades del MCD:

Si $a, b, n, m \in \mathbb{Z}$, entonces:

- Si $mcd(a, n) = mcd(b, n) = 1$, entonces $mcd(ab, n) = 1$.
- Si $c|ab$ y $mcd(b, c) = 1$, entonces $c|a$.
- $mcd(ma, mb) = m[mcd(a, b)]$.
- Si $d|a$ y $d|b$ y $d > 0$, entonces $mcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} mcd(a, b)$.
- $mcd(a, b) = mcd(a, b \pm an)$. Esta propiedad nos da el algoritmo de Euclides.

Ejercicio: Demostrar las propiedades anteriores a excepción de la última.

Obtención del MCD factorizando por primos:

El MCD de dos números a y b tiene una factorización por primos en la que cada primo p divide tanto a a como a b, y el exponente de p es el más pequeño de los exponentes de p en las factorizaciones de a y de b. Es decir, el MCD se construye usando los primos divisores comunes de a y b, con el menor de los exponentes en las factorizaciones de a y b.

Ejemplos: $56 = 2 \cdot 2 \cdot 2 \cdot 7 = 2^3 \cdot 7$ y $140 = 2 \cdot 2 \cdot 5 \cdot 7 = 2^2 \cdot 5 \cdot 7$.

Entonces $mcd(56,140) = 2^2 \cdot 7 = 28$.

Ejemplo: $375 = 3 \cdot 5 \cdot 5 \cdot 5 = 3 \cdot 5^3$ y $450 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 = 2 \cdot 3^2 \cdot 5^2$.

Entonces $mcd(375,450) = 3 \cdot 5^2 = 75$.

Ejemplo: Para obtener $mcd(48,60)$, obtenemos la factorización de cada número:

48	2
24	2
12	2
6	2
3	3
1	

$48 = 2^4 \cdot 3$

60	2
30	2
15	3
5	5
1	

$60 = 2^2 \cdot 3 \cdot 5$

2 y 3 son los factores comunes de 48 y 60. Y el menor exponente de cada uno de los factores comunes es 2 y 1, respectivamente. Entonces, $mcd(48,60) = 2^2 \cdot 3 = 12$.

4. Primos relativos

En el material anterior de números se mencionó que los primos relativos son aquellos números que no tienen factores en común en su descomposición canónica o factorización por primos. Otra forma de definir a los primos relativos es utilizando el máximo común divisor. Si a y $b \in \mathbb{Z}$ tales que $mcd(a,b) = 1$, entonces decimos que a y b son **primos relativos** o **primos entre sí.**

Ejemplo: $mcd(21,40) = 1$, por lo tanto, son primos relativos. Esto puede comprobarse, observando la descomposición canónica de cada número:

$$21 = 3 \times 7$$

$$40 = 2^3 \times 5$$

No presentan factores en común, por lo que comprobamos que son primos relativos.

5. Datos de vital importancia

1. Euler no le caía bien a Federico el Grande, quien lo apodó “El cíclope matemático” por haber perdido el ojo derecho a los 30 años. https://elibro.net/es/ereader/uaa/127786?page=154
2. El rectángulo áureo (aquél que al quitarle un cuadrado nos da otro rectángulo áureo) es la base de la arquitectura helénica. https://elibro.net/es/lc/uaa/titulos/37796

6. Mínimo común múltiplo

Decimos que m es el **mínimo común múltiplo (mcm)** de dos números naturales a y b, y se escribe $m = mcm(a,b)$, si se cumplen las siguientes condiciones:

1. $a|m$ y $b|m$, es decir, m es un múltiplo de a y de b.
2. n es tal que $a|n$ y $b|n$, entonces $m \leq n$; es decir, no existe un múltiplo de a y b que sea menor que m.

En otras palabras, el mínimo común múltiplo de a y b es el menor entero positivo que es múltiplo de estos dos números.

Otra notación utilizada para expresar el mínimo común múltiplo de dos números a y b es $[a,b]$.

Algunas propiedades del mcm:

- Si $l = mcm(a,b)$ y m es un múltiplo común de a y b, entonces $l|m$.
- Si $m > 0$, entonces $mcm(ma,mb) = m \cdot [mcm(a,b)]$.
- Se tiene que $mcd(a,b) \cdot mcm(a,b) = ab$.

Ejercicio: Demostrar las propiedades anteriores.

Obtención del mcm factorizando por primos:

El mcm de dos números a y b tiene una factorización por primos en la que cada primo p divide a a o a b, y el exponente de p es el mayor de los exponentes que p presenta en las factorizaciones de a o de b. Es decir, el mcm se construye usando todos los primos divisores a o de b, utilizando el mayor de los exponentes que aparecen en las factorizaciones de a o b.

Ejemplo: $28 = 2 \cdot 2 \cdot 7 = 2^2 \cdot 7$ y $48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$.

Entonces $mcm(28,48) = 2^4 \cdot 3 \cdot 7 = 336$.

Ejemplo: $135 = 3 \cdot 3 \cdot 3 \cdot 5 = 3^3 \cdot 5$ y $450 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 = 2 \cdot 3^2 \cdot 5^2$.

Entonces $mcm(135,450) = 2 \cdot 3^3 \cdot 5^2 = 1350$.

Ejemplo: Para encontrar $mcm(180,324)$, obtenemos la factorización de cada número:

180	2
90	2
45	5
9	3
3	3

$180=2^2\times5\times3^2$

324	2
162	2
81	3
27	3
9	3
3	3

$324=2^2\times3^4$

Ya que obtuvimos la factorización por primos de 180 y 324, $mcm(180,324) = 2^2 \cdot 3^4 \cdot 5 = 1620$.

7. Algoritmo de Euclides

Aunque el método por factorización es eficaz para obtener el máximo común divisor, en ocasiones la factorización por primos se puede complicar. Por ejemplo, si quisiéramos calcular el valor de (a, b), podríamos seguir el proceso antes mencionado $(a, b) = (a - b, b) = (a - 2b, b) = \cdots = (a - bn, b)$, donde $0 \leq a - bn \leq b$. Pero este proceso se complica cuando el valor de n es muy grande. Para eso podemos usar el algoritmo de la división: sabemos que al dividir dos enteros positivos a y b, con $b \neq 0$, existe un par de enteros q y r tales que $a = bq + r$ y $0 \leq r < b$. Por lo tanto, $(a, b) = (bq + r, b) = (bq + r - bq, b) = (r, b)$.

El algoritmo presentado aparece en el libro VII de *Los Elementos*, el cual es una recopilación hecha por Euclides de los conocimientos matemáticos griegos alrededor del año 300 a.C. Por esta razón es que a este método se le conoce como el **Algoritmo de Euclides**.

Retomando el algoritmo de la división, por comodidad al residuo r de la división de a entre b lo simbolizaremos como $r = res(a, b)$, $a = r_0$ y $b = r_1$.

El algoritmo de Euclides es el siguiente:

Calculamos $r_2 = res(r_0, r_1)$, si $r_2 = 0$ entonces $r_1 = mcd(a, b)$, en caso contrario calculamos $r_3 = res(r_1, r_2)$, si $r_3 = 0$ entonces $r_2 = mcd(a, b)$, en caso contrario calculamos $r_4 = res(r_2, r_3)$, si $r_4 = 0$ entonces $r_3 = mcd(a, b)$, en caso contrario continuamos este procedimiento hasta llegar a un residuo que sea 0. Si $r_n = 0$ entonces $r_{n-1} = mcd(a, b)$. Como los residuos cada vez se hacen más pequeños, este procedimiento acabará. En caso de que sean negativos los números, se puede aplicar este método a los valores absolutos de los mismos.

Ejemplo: Obtener el máximo común divisor de 66 y 42.

El residuo que se obtiene al dividir 66 entre 42 es 24.

El residuo que se obtiene al dividir 42 entre 24 es 18.

El residuo que se obtiene al dividir 24 entre 18 es 6.

El residuo que se obtiene al dividir 18 entre 6 es 0.

Por lo tanto, (66,42)=6.

8. Problemas:

1. Demuestra que el producto de 3 enteros consecutivos siempre es divisible entre 6.
2. Demuestra que, si x y y son impares, entonces $x^2 + y^2$ no es divisible entre 4.
3. Calcula $mcd(72,48)$ y $mcm(72,48)$.
4. Calcula $mcd(561,3003)$ y $mcm(561,3003)$.
5. Demuestra que si $mcd(a,b) = 1$ y $c|a$, entonces $mcd(c,b) = 1$.
6. Si $mcd(a,b) = 8$, ¿cuáles son los posibles valores de $mcd(a^3, b^4)$?
7. Demuestra que para cualquier número n entero se cumple que n y $n+1$ son primos relativos o primos entre sí.
8. Suponga que $(a,b,c) = 1$ y que $\frac{ab}{a-b} = c$. Demuestra que $a-b$ es un cuadrado perfecto.
9. Demuestra que $(n! + 1, (n+1)! + 1) = 1$.
10. Sean a y b enteros positivos tales que $a = bq + r$ con $0 \leq r < b$. Demuestra que $(2^a - 1, 2^b - 1) = (2^b - 1, 2^r - 1) = 2^{(a,b)} - 1$.