

# Divisibilidad

## OMMJAL- Femenil

EMMANUEL BUENROSTRO

5 April 2025

### §1 Definiciones

**Definition 1.1** (Divisibilidad). Sean  $a, b$  enteros, decimos que  $a \mid b$  si existe un entero  $x$  tal que  $b = ax$ .

**Definition 1.2** (Valor absoluto). El valor absoluto de un número  $a$  es

$$|a| = \begin{cases} a & \text{si } a \geq 0, \\ -a & \text{si } a < 0. \end{cases}$$

Que se suele ver como la distancia al origen de ese punto  $a$  en la recta real, o bastante menos formalmente visto como "el número pero sin signo".

**Propiedades:** Para  $a, b, c, r, s$  enteros

1.  $a \mid b$  si y solo si  $|a| \mid |b|$
2. Si  $a \mid b$  entonces  $|a| \leq |b|$  (Para  $b \neq 0$ )
3.  $a \mid a$
4.  $1 \mid a$
5.  $a \mid 0$  ( Porque  $0 = a \cdot 0$  )
6. Si  $a \mid b$  y  $b \mid a$  entonces  $|a| = |b|$
7. Si  $a \mid b$  y  $a \mid c$  entonces  $a \mid rb + sc$  para cualesquiera  $r, s$  enteros.
8. Si  $\text{mcd}(a, b) = 1$  y  $a \mid bc$  entonces  $a \mid c$

**Remark 1.3** (No es si y solo si). No es un si y solo si, es decir si  $a \mid c$  y  $a \mid bc$ , no necesariamente  $\text{mcd}(a, b) = 1$ . Ejemplo de esto es  $2 \mid 4$  y  $2 \mid 6 \cdot 4$  pero  $\text{mcd}(2, 6) \neq 1$

9. Si  $a \mid b$  entonces  $a \mid bc$  para todo entero  $c$ . (Caso particular del 7)

De aqui surgen estos dos conceptos

**Definition 1.4.** El maximo comun divisor de dos enteros  $a, b$  (usualmente escrito solo como  $\text{mcd}(a, b)$  o  $\text{gcd}(a, b)$  por su nombre en ingles) es el maximo entero positivo  $d$  tal que

$$d \mid a \text{ y } d \mid b$$

. Notemos que este siempre existe porque 1 divide a ambos números.

**Definition 1.5.** El mínimo común múltiplo de dos enteros  $a, b$  (usualmente escrito solo como  $\text{mcm}(a, b)$  o  $\text{lcm}(a, b)$  por su nombre en inglés) es el mínimo entero positivo  $d$  tal que

$$a|d \text{ y } b|d$$

. Notemos que este siempre existe porque  $d = ab$  cumple para ambos números.

Por ejemplo para  $a = 12, b = 18$  se tiene que  $\text{mcd}(12, 18) = 6$  y  $\text{mcm}(12, 18) = 36$ .

## §1.1 Ejercicios

**Exercise 1.6.** ¿Para cuales enteros positivos  $n$  se tiene que  $n|n + 14$  ?

**Exercise 1.7.** ¿Para cuales enteros positivos  $n$  se tiene que  $n|n + 1$  ?

**Exercise 1.8.** ¿Para cuales enteros positivos  $n$  se tiene que  $2025n|n + 2025$  ?

**Exercise 1.9.** ¿Para cuales enteros positivos  $n$  se tiene que  $n + 2025|2025n$  ?

**Exercise 1.10.** ¿Para cuales enteros positivos  $n$  se tiene que  $n - 1|n^2 - 2$  ?

## §2 Lema de la Division de Euclides

Vamos a considerarnos el conjunto de múltiplos de 5 no negativos.

$$\{0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, \dots\}$$

Entonces, ¿Qué pasa con los números como 32, 33 que no estan en ese conjunto?, pues estan en medio entre 30 y 35, entonces podemos escribirlos como

$$32 = 5 \times 6 + 2$$

$$33 = 5 \times 6 + 3$$

$$34 = 5 \times 6 + 4$$

$$35 = 5 \times 6 + 5$$

$$36 = 5 \times 6 + 6$$

Pero 35 y 36 ya no estan en medio de 30 y 35 entonces mejores formas de escribirlos seria

$$35 = 5 \times 7 + 0$$

$$36 = 5 \times 7 + 1$$

Siguiendo esto obtenemos el lema:

### Lemma 2.1 (Lema de la Division de Euclides)

Para cualesquiera enteros  $a, b$  podemos encontrar **únicos** enteros  $q, r$  tales que

$$b = aq + r$$

con  $0 \leq r < a$ , donde  $q$  es el cociente y  $r$  el residuo.

### §3 Algoritmo de la División de Euclides

#### Lemma 3.1

Sean  $a, b$  enteros. Si escribimos  $a = bq + r$  para enteros  $q, r$  con  $0 \leq r < b$  entonces

$$\text{mcd}(a, b) = \text{mcd}(r, b)$$

*Proof.* Notemos que  $\text{mcd}(a, b) \mid b$  y como  $\text{mcd}(a, b) \mid a = bq + r \Rightarrow \text{mcd}(a, b) \mid r$  Entonces  $\text{mcd}(a, b) \mid \text{mcd}(r, b)$

Y además

$$\text{mcd}(r, b) \mid b \text{ y } \text{mcd}(r, b) \mid r = a - bq \Rightarrow \text{mcd}(r, b) \mid a \Rightarrow \text{mcd}(r, b) \mid \text{mcd}(a, b)$$

Entonces como ambos son positivos  $\text{mcd}(a, b) = \text{mcd}(r, b)$  □

Entonces, el algoritmo de la división es aplicar esto hasta que en algún punto llegas a que un número divide a otro, siendo el menor tu resultado.

Veamos un ejemplo, para calcular  $\text{mcd}(370, 100)$  queda:

$$\text{mcd}(370, 100) = \text{mcd}(70, 100) = \text{mcd}(70, 30) = \text{mcd}(10, 30) = 10$$

porque  $10 \mid 30$ .

#### ¿Pero por qué termina?

Esto sucede porque en cada paso el residuo es menor, entonces eventualmente llega a 0 (y cuando llega a 0 en el paso anterior un número dividía a otro).

#### §3.1 Ejercicios

**Exercise 3.2.** Calcula  $\text{mcd}(124, 440)$  usando el algoritmo.

**Exercise 3.3.** Demuestra que  $\text{mcd}(4n + 3, 2n) \in \{1, 3\}$ .

### §4 Bezout

Ahora vamos a centrarnos en expresiones de la forma

$$ax + by = n$$

Para  $a, b$  enteros fijos,  $x, y, n$  enteros.

#### §4.1 ¿Cuáles $n$ son posibles?

Notemos que  $\text{mcd}(a, b) \mid ax + by = n$ , entonces  $n$  es múltiplo de  $\text{mcd}(a, b)$ .

## §4.2 Construcción

Entonces veremos cuales multiples de  $\text{mcd}(a, b)$  son posibles, y la respuesta es que todos. Para eso vamos a ver que existen  $x, y$  con  $ax + by = \text{mcd}(a, b)$ .

Entonces notemos que el proceso de el algoritmo de Euclides es totalmente reversible, pero para eso vamos a escribirlo de una forma más extensa usando el mismo ejemplo de  $\text{mcd}(370, 100)$ .

$$370 = 100 \times 3 + 70$$

$$100 = 70 \times 1 + 30$$

$$70 = 30 \times 2 + 10$$

Y entonces veamos que

$$10 = 70 \cdot 1 - 30 \cdot 2$$

Entonces usando el paso anterior  $30 = 100 \cdot 1 - 70 \cdot 1$  y

$$10 = 70 \cdot 1 - (100 \cdot 1 - 70 \cdot 1) \cdot 2 = 70 \cdot 3 - 100 \cdot 2$$

Y en el paso anterior  $70 = 370 \cdot 1 - 100 \cdot 3$  y

$$10 = (370 \cdot 1 - 100 \cdot 3) \cdot 3 - 100 \cdot 2 = 370 \cdot 3 - 100 \cdot 11$$

Entonces ya escribimos 10 como una combinacion lineal de 370 y 100.

Y en general podemos regresar los pasos del algoritmo de la división para encontrar los  $x, y$  tales que

$$ax + by = \text{mcd}(a, b)$$

**Exercise 4.1.** Ahora demuestra que si existen para todos los multiples de  $\text{mcd}(a, b)$

## §5 Factorización Canonica

**Definition 5.1 (Primo).** Un número entero  $p$  es primo si sus unicos divisores son 1,  $p$ , en particular 1 no es primo. (Si consideras divisores negativos entonces los unicos son  $-a, -1, 1, a$  y  $1, 0, -1$  no son primos.

Los primeros primos son: 2,3,5,7,11,13,17,19,23,29.  
En particular el unico primo par es 2.

Los números primos solo los divide si mismo y 1, osea solo un primo.  
Los números compuestos los dividen dos o más primos (contando multiplicidad, es decir puede ser dos veces el mismo primo).

### Theorem 5.2 (Teorema Fundamental de la Aritmetica)

El TFA nos dice que todo numero natural tiene una representacion unica como producto de potencias de primos (Esta es la factorización canonica). Es decir

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$$

Donde cada  $p_i$  es primo elevado a una potencia entera  $\alpha_i$ .

Esto sirve para muchísimas cosas, voy a mostrar solo unas cuantas.

Por ejemplo para saber si un número  $x$  es una  $n$ -ésima potencia. Para esto ocupamos que cada uno de los exponentes de la factorización canónica de  $x$  sea múltiplo de  $n$ . Porque justo al elevar un número a la  $n$  lo que estas haciendo es multiplicar todas sus potencias por  $n$ .

Por ejemplo  $36 = 2^2 \cdot 3^2$  y como todos los exponentes son múltiplos de 2, entonces 36 es un cuadrado perfecto.

Esto también lo puedes hacer para saber por qué valor tienes que multiplicar para llegar a cierta potencia. Por ejemplo el menor entero positivo  $x$  tal que  $72x$  es un cubo perfecto se puede obtener viendo que  $72 = 2^3 \cdot 3^2$  y quieres que todos sean múltiplos de 3, entonces solo te falta multiplicar por un 3 para que se vuelva  $72 \cdot 3 = 2^3 \cdot 3^3$  y eso ya es un cubo.

Para saber si un número  $a$  divide a  $b$ , la factorización canónica de  $a$  debe de estar "contenida" en la de  $b$ , donde estar contenida es que todos los primos que aparecen en la de  $a$ , aparecen en la de  $b$  y tienen un exponente menor o igual al que esta en  $b$ , mas formalmente. Si  $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$  y  $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ , entonces  $a|b \iff$

$$\alpha_i \leq \beta_i \quad \forall 1 \leq i \leq k$$

**Exercise 5.3.** ¿ $2^9 \cdot 3^3$  es divisible por  $2 \cdot 3$  ?

**Exercise 5.4.** ¿ $2^9 \cdot 3^3$  es divisible por  $2^8 \cdot 3^8$  ?

**Exercise 5.5.** ¿ $2^9 \cdot 3^3$  es divisible por  $2 \cdot 3 \cdot 5$  ?

**Exercise 5.6.** ¿ $2^9 \cdot 3^3$  es divisible por  $2 \cdot 3^8$  ?

**Exercise 5.7.** ¿ $2^9 \cdot 3^3$  es divisible por  $3^3$  ?

También podemos relacionar el mcd, mcm con esta factorización canónica.

Si  $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$  y  $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ , entonces

$$\text{mcd}(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}$$

y

$$\text{mcm}(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}$$

**Exercise 5.8.** Prueba que para cualesquiera dos enteros  $a, b$  se tiene que

$$\text{mcd}(a, b) \cdot \text{mcm}(a, b) = ab$$

Y sobretodo, todo esto te sirve para poder caracterizar y trabajar con los números de forma algebraica.

No tengo razones para exigirte ni apresurarte, pero aun así no cambia el hecho de que lo quería

Iker esperando el correo de Lalo

## §6 Problemas Parte 1

Los problemas no estan necesariamente en orden de dificultad.

**Problem 6.1.** Si un entero  $A$  no es mutiplo de 3 puede  $2A$  serlo?

**Problem 6.2.** Halla el menor entero positivo  $x$  tal que  $8x$  es un cuadrado perfecto y  $12x$  es un cubo perfecto.

**Problem 6.3.** Encuentra el menor entero positivo por el que hay que multiplicar 18 para que sea un cubo perfecto.

**Problem 6.4.** Al contar unos ladrillos se dieron cuenta que de 2 en 2 sobraba 1, de 3 en 3 tambien , de 5 en 5 tambien, de 7 en 7 tambien. ¿Cuál es la minima cantidad de ladrillos que puede haber?

**Problem 6.5.** El número de alumnos en un colegio esta entre 500 y 1000. Si se cuentan de 3 en 3 no sobra ninguno, y si se cuentan de 5 en 5 tampoco. Si el número de alumnos de cada salon es igual al numero de salones, halla el número de alumnos en el colegio.

**Problem 6.6.** ¿Cuántos divisores positivos tiene el número  $20!$ ?

**Problem 6.7.** ¿Cuántos divisores positivos tiene un número  $n$ ? (puedes decirlo en base a su factorizacion canonica)

**Problem 6.8.** Demuestra que la fracción

$$\frac{21n + 4}{14n + 3}$$

es irreducible para todo entero  $n$ .

**Problem 6.9.** ¿En cuántos ceros termina  $2025!$ ?

**Problem 6.10.** Demuestre que la fracción  $\frac{n^2+n-1}{n^2+2n}$  es irreducible para todo entero positivo  $n$ .

## §7 Problemas Parte 2

Los problemas no estan necesariamente en orden de dificultad.

Si resuelves al menos 6 problemas de esta parte dime y te mando la parte 3.

**Problem 7.1.** Probar que  $5 \mid 2n + 3m$  si y solo si  $5 \mid n + 4m$ .

**Problem 7.2.** Demuestra que para  $n$  natural y  $a, b$  enteros cualesquiera

$$a - b \mid a^n - b^n$$

Y si  $n$  impar entonces

$$a + b \mid a^n + b^n$$

**Problem 7.3.** Encuentra 100 numeros consecutivos tales que ninguno sea primo.

**Problem 7.4.** Si  $a$  y  $b$  son enteros positivos, demostrar que  $11a + 2b$  es múltiplo de 19 si y sólo si lo es  $18a + 5b$ .

**Problem 7.5.** Prueba que si  $p$  es primo y  $0 < k < p$ , entonces  $\binom{p}{k}$  es divisible por  $p$ .

**Problem 7.6.** Demuestra que  $n$  no es primo si y solo si existe algun primo  $p \leq \sqrt{n}$  con  $p \mid n$ .

**Problem 7.7.** Sean  $a$  y  $b$  enteros positivos tales que

$$\frac{5a^4 + a^2}{b^4 + 3b^2 + 4}$$

es un número entero. Demuestra que  $a$  no es un número primo.

**Problem 7.8.** Sea  $n$  un entero positivo y sean  $d_1, d_2, \dots, d_k$  los divisores de  $n$  escritos de menor a mayor. Sean

$$C = d_1 d_k^2 + d_2 d_{k-1}^2 + \dots + d_{k-1} d_2^2 + d_k d_1^2$$

$$S = d_1 + d_2 + \dots + d_{k-1} + d_k$$

Determina  $\frac{C}{S}$  en terminos de  $n$ .

**Problem 7.9.** Prueba que la expresión

$$\frac{\text{mcd}(m, n)}{n} \binom{n}{m}$$

es entero para cualquier pareja de enteros  $n \geq m \geq 1$ .

**Problem 7.10.** Determina todos los enteros compuestos  $n > 1$  que cumplen lo siguiente: si  $d_1, d_2, \dots, d_k$  son todos los divisores positivos de  $n$  con  $1 = d_1 < d_2 < \dots < d_k = n$ , entonces  $d_i$  divide a  $d_{i+1} + d_{i+2}$  para todo  $1 \leq i \leq k - 2$ .

## §8 Parte 3

Puedes intentar los problemas de esta parte, aunque tal vez es mejor que termines la mayoría de los problemas de las partes anteriores.

Los problemas no están en orden de dificultad.

Si te acabas estos problemas dime y te mando más.

**Problem 8.1.** Encuentra todos los enteros positivos  $n$  tales que  $3n - 4$ ,  $4n - 5$  y  $5n - 3$  son todos primos.

**Problem 8.2.** Sean  $m, n$  enteros positivos tales que

$$\text{mcd}(m, n) + \text{mcm}(m, n) = m + n$$

Entonces uno de los dos números es divisible por el otro.

**Problem 8.3.** Encuentra todos los enteros positivos  $n$  tales que

$$3^{n-1} + 5^{n-1} \mid 3^n + 5^n$$

**Problem 8.4.** Un número  $x$  es Tlahiuca si existen primos positivos distintos  $p_1, p_2, \dots, p_k$  tales que

$$x = \frac{1}{p_1} + \frac{1}{p_2} + \dots + \frac{1}{p_k}.$$

Determina el mayor número Tlahiuca  $x$  que satisface las dos siguientes propiedades:

- $0 < x < 1$ .
- Existe un número entero  $0 < m \leq 2022$  tal que  $mx$  es un número entero.

**Problem 8.5.** Determina todos los pares  $(a, b)$  de enteros que satisfacen ambas condiciones:

- $5 \leq b < a$
- Existe un número natural  $n$  tal que los números  $\frac{a}{b}$  y  $a - b$  son divisores consecutivos de  $n$  en ese orden.

**Problem 8.6.** Sea  $n > 1$  un entero positivo y sean  $d_1 < d_2 < \dots < d_m$  sus  $m$  divisores positivos de manera que  $d_1 = 1$  y  $d_m = n$ . Lalo escribe los siguientes  $2m$  números en un pizarrón:

$$d_1, d_2, \dots, d_m, d_1 + d_2, d_2 + d_3, \dots, d_{m-1} + d_m, N$$

donde  $N$  es un entero positivo. Después Lalo borra los números repetidos (por ejemplo, si un número aparece dos veces, él borrará uno de los dos). Después de esto, Lalo nota que los números en el pizarrón son precisamente la lista completa de divisores positivos de  $N$ . Encuentra todos los posibles valores del entero positivo  $n$ .

**Problem 8.7.** Sean  $n, p > 1$  enteros positivos con  $p$  primo. Dado que  $n \mid p - 1$  y  $p \mid n^3 - 1$ , prueba que  $4p - 3$  es un cuadrado perfecto.

**Problem 8.8.** Para cada entero positivo  $n$ , sea  $d(n)$  la cantidad de divisores positivos de  $n$ .

Prueba que para todas las parejas de enteros positivos  $(a, b)$  se cumple que

$$d(a) + d(b) \leq d(\text{mcd}(a, b)) + d(\text{mcm}(a, b))$$

Y determina cuáles parejas  $(a, b)$  cumplen el caso de igualdad.