Divisibilidad

Alan Reyes-Figueroa

Teoría de Números (Aula 02) 13.julio.2021

Divisibilidad

Definición

Dados dos enteros $d, m \in \mathbb{Z}$ diremos que d ***divide*** *a m o que m es* ***divisible*** *entre m si existe $q \in \mathbb{Z}$ tal que $m = qd$, esto es $\frac{m}{d} \in \mathbb{Z}$ es un entero.*
En ese caso, escribimos $d \mid m$, y diremos que m es un ***múltiplo*** *de d, y que d es un* ***divisor*** *o* ***factor*** *de m.*
Si d no divide a m escribimos $d \nmid m$.

Ejemplos: $5 \mid 10$, pero $10 \nmid 5$.

Como $0 = 0 \cdot n$ se sigue que $n \mid 0$, $\forall n \in \mathbb{Z}$. Por otro lado, si $0 \mid n$, entonces existe $q \in \mathbb{Z}$ tal que $n = q \cdot 0 = 0$, de modo que $0 \nmid n$ para $n \neq 0$. Para un entero fijo n, los múltiplos de n son $0, \pm n, \pm 2n, \ldots$. Luego, no es difícil ver que entre n enteros consecutivos, siempre hay uno divisible entre n.

Propiedades

Para todo $x, y, z, w \in \mathbb{Z}$, *valen*

a) $x \mid 0$, $1 \mid x$, $0 \nmid x$ *para* $x \neq 0$; $x \mid x$ *(reflexividad).*

b) $x \mid 1$, *si y sólo si,* $x = \pm 1$.

c) $x \mid y, y \mid z \;\Rightarrow\; x \mid z$ *(transitividad).*

d) $x \mid y, x \mid z \;\Rightarrow\; x \mid ay + bz$, *para todo* $a, b \in \mathbb{Z}$ *(linealidad).*

e) *Si* $x \mid y$, *entonces* $y = 0$ *ó* $|x| \leq |y|$ *(limitación).*

f) $x \mid y, x \mid y \pm z \;\Rightarrow\; x \mid z$.

g) $x \mid y, y \mid x \;\Rightarrow\; |x| = |y|$ *(antisimetría, a menos de signo).*

h) *Si* $x \mid y$ *y* $y \neq 0$, *entonces* $\frac{y}{x} \mid y$ *(divisores vienen en pares).*

i) $x \mid y, z \mid w \;\Rightarrow\; xz \mid yw$.

j) *Si* $z \neq 0$, *entonces* $x \mid y \;\Leftrightarrow\; xz \mid yz$.

Prueba: (a) Observe que $x = 1 \cdot x$, $0 = x \cdot 0$, $0 \mid x \ \Rightarrow x = q \cdot 0 = 0$; $x = x1$.
Para (b) $x \mid 1 \ \Leftrightarrow \ 1 = qx, \in \mathbb{Z} \ \Leftrightarrow \ q = \pm 1$, y portanto $x = \pm 1$.

En los ítems (c) a (h), la condición $x \mid y$ se da, de modo que $y = kx$, para algún $k \in \mathbb{Z}$.
En (c) $y \mid z \ \Rightarrow \ z = \ell y \ \Rightarrow \ z = \ell y = \ell(kx) = (k\ell)x$, con $k\ell \in \mathbb{Z} \ \Rightarrow x \mid z$.

En (d) $x \mid z \ \Rightarrow \ z = \ell x \ \Rightarrow \ ay + bz = a(kx) + b(\ell x) = (ak + b\ell)x \ \Rightarrow \ x \mid ay + bz$.

En (e), suponga $y \neq 0$. Entonces $k \neq 0 \ \Rightarrow \ |k| \geq 1 \ \Rightarrow |y| = |kx| = |k| \cdot |x| \geq |x|$.

En (f), por (c) tenemos que $x \mid y$, $x \mid y \pm z \ \Rightarrow \ x \mid y - (y \pm z) = \pm z$.

En (g), de (e) se tiene que $x \mid y$, $y \mid x \ \Rightarrow \ |y| \geq |x| \geq |y| \ \Rightarrow \ |y| = |x|$.

En (h), si $y \neq 0$, entonces $x \mid y \ \Rightarrow y = kx = (\frac{y}{x})x$. Como $\frac{y}{x} \in \mathbb{Z} \ \Rightarrow \ \frac{y}{x} \mid y$.

En (i), $y = kx$, $w = \ell z \ \Rightarrow yw = (kx)(\ell z) = (k\ell)xz \ \Rightarrow \ xz \mid yw$.

Finalmente (j), ($\Rightarrow$) de (i) con $w = z$, se tiene que $x \mid y$, $z \mid z \ \Rightarrow \ xz \mid yz$. Para la recíproca
($\Leftarrow$) $xz \mid yz$, $z \neq 0 \ \Rightarrow \ xz = k(yz) = kxz, \ k \in \mathbb{Z} \ \Rightarrow \ x = ky \ \Rightarrow \ x \mid y$. $\square$

Comentarios:

- Las propiedades (a), (c) y (g), corresponden a la reflexividad, transitividad y antisimetría (a menos de signo) de la relación $|$. Restricta a los naturales $\mathbb{N}$, la relación $|$ es un **orden parcial**.
- La propiedad (d) de linealidad sólo funciona para coeficientes en $\mathbb{Z}$.
- La propiedad (j) indica que en una relación de divisibilidad, podemos "cancelar" factores comunes (excepto 0).
- La (e), limitación, nos dice que el conjunto de divisores de un número entero n es finito. El número de divisores positivos de n es $\leq n$.
- La propiedad (h) nos indica que los divisores de n vienen en pares $(d, \frac{n}{d})$. **Obs!** No dice que los divisores d y $\frac{n}{d}$ son distintos.

Ejemplo: 99 estudiantes aburridos se turnan para caminar por un pasillo que contiene una fila de casilleros cerrados, numerados del 1 al 99. El primer estudiante abre todos los casilleros; el segundo alumno cierra todos los casilleros numerados $2, 4, 6, 8, \ldots, 98$; el tercer alumno opera en los casilleros numerados $3, 6, 9, \ldots, 99$: si un casillero estaba cerrado, lo abre, y si un casillero estaba abierto, lo cierra. Para el k-ésimo alumno, trabaja en los casilleros numerados por múltiplos de k: si un el casillero estaba cerrado, lo abre, y si estaba abierto, lo cierra.
¿Cuál es el número de casilleros que permanecen abiertos después de que todos los estudiantes terminan sus caminatas?

Respuesta: 1, 4, 9, 16, 25, 36, 49, 64, 81.

Ejemplo: Hallar todos los enteros positivos n tales que $2n^2 + 1 \mid n^3 + 9n - 17$.

Ejemplo: Pruebe que para todo entero positivo n, la fracción $\frac{21n+4}{14n+3}$ es irreducible.

Ejemplo: Mostrar que para todo entero n:

a) $n^5 - 5n^3 + 4n$ es divisible entre 120.

b) $n^2 + 3n + 5$ no es divisible por 121.

Ejemplo: Encontrar todos los enteros positivos n para los cuales el número obtenido de n al borrar el último dígito, es un divisor de n.

Ejemplo: ¿Cuál es la mayor entero positivo x tal que $23^x \mid 2021!$?

Algoritmo de la División

El siguiente resultado juega un papel muy importante en la teoría de números.

Teorema (Algoritmo de la División)

Para cualesquiera enteros $a, b \in \mathbb{Z}$, $a > 0$, existe un único par (q, r) de enteros, tales que

$$b = qa + r, \quad y \quad 0 \leq r < a. \tag{1}$$

*En este caso, q es llamado **cociente** y r el **residuo** al dividir b entre a.*

Prueba: La prueba consiste de dos parte: la existencia y la unicidad. Para la existencia, mostramos que el conjunto

$$S = \{b - xa : x \in \mathbb{Z},\ b - xa \geq 0\},$$

es no vacío. Para ello, mostramos un valor de x para el cual $b - xa \geq 0$.

Como $a \geq 1$, entonces $|b|a \geq |b| \;\Rightarrow\; b - (-|b|)a = b + |b|a \geq b + |b| \geq 0$. Así, para $x = -|b|$, el entero $b - xa \in S$.

Aplicando el Principio de buen orden, entonces S posee un elemento mínimo r. En particular, existe $q \in \mathbb{Z}$ tal que $r = b - qa \geq 0$. Mostramos $r < a$. Si este no fuera el caso, entonces $r \geq a$ y $b - (q+1)a = (b - qa) - a = r - a \geq 0$ sería un elemento de S. Pero $b - (q+1)a < b - qa = r$, lo que contradice la minimalidad de r. Por lo tanto, $r < a$, y hemos probado que existen $q, r \in \mathbb{Z}$, con la propiedad (1).

Para mostrar la unicidad, suponga que existen dos representaciones en la forma deseada

$$b = qa + r = q'a + r', \quad \text{con} \quad 0 \leq r < a,\; 0 \leq r' < a.$$

Entonces, $r' - r = (q - q')a$. En particular, $|r' - r| = |q - q'|\, a$.

Algoritmo de la División

Por otro lado, como $0 \leq r < a$ entonces $-a < -r \leq 0$. Sumándola con la otra desigualdad $0 \leq r' < a$, obtenemos que la diferencia de residuos satisface $-a < r' - r < a \;\Rightarrow\; |r' - r| < a$. Entonces

$$0 \leq |q - q'|\,a = |r' - r| < a \;\text{ implica que }\; 0 \leq |q - q'| < 1.$$

Siendo q, q' ambos enteros, entonces $q - q'$ es también un entero. La desigualdad $0 \leq |q - q'| < 1$ implica que la única posibilidad es que $q - q' = 0 \;\Rightarrow\; q' = q$. De ahí que $r' - r = (q - q')a = 0 \cdot a = 0$ y $r' = r$. Esto muestra la unicidad de la representación. $\square$

Algoritmo de la División

Una versión más general del algoritmo es la siguiente:

Corolario (Algoritmo de la División)

Para cualesquiera enteros $a, b \in \mathbb{Z}$, $a \neq 0$, existe un único par (q, r) de enteros, tales que

$$b = qa + r, \quad y \quad 0 \leq r < |a|. \tag{2}$$

Prueba: Basta considerar el caso $a < 0$. Entonces $|a| > 0$ y el algoritmos de la división en (1) establece que existen únicos $q, r \in \mathbb{Z}$ tales que $b = q|a| + r$, con $0 \leq r < |a|$.
Como $a < 0$, entonces $b = q|a| + r = (-q)a + r$, $0 \leq r < |a|$ satisface (2). $\square$

Ejemplo: Para ilustrar el algoritmo de la división, tome $a = 13$, $b = 61$.

Algoritmo de la División

Tenemos que

$$61 = 4 \cdot 13 + 9, \quad \text{con} \quad 0 \leq 9 < 13.$$

Observe que el algoritmo de la división equivale a hacer la "división tradicional" de $\frac{61}{13}$ a mano: $q = 4$ resulta el cociente, y 9 resulta ser el residual.

Esto también equivale a hacer $\frac{61}{13} = 4 + \frac{9}{13}$: pues

$$b = qa + r \;\Leftrightarrow\; \frac{b}{a} = q + \frac{r}{a}.$$

Ejemplo: Para ilustrar el algoritmo con $a < 0$, tomemos $a = -7$:

- Con $b = 1$: $1 = (0)(-7) + 1 \;\Rightarrow\; q = 0, r = 1$.
- Con $b = -2$: $-2 = 1(-7) + 5 \;\Rightarrow\; q = 1, r = 5$.
- Con $b = 60$: $60 = (-8)(-7) + 4 \;\Rightarrow\; q = -8, r = 4$.
- Con $b = -60$: $-60 = 9(-7) + 3 \;\Rightarrow\; q = 9, r = 3$.

Algoritmo de la División

Ejemplo: Sea $n \in \mathbb{Z}^+$. Probar que $3^{2^n} + 1$ es divisible por 2, pero no por 4.

Solución: 3^{2^n} es impar y $3^{2^n} + 1$ es par. Observe que
$3^{2^n} = \left(3^2\right)^{2^{n-1}} = 9^{2^{n-1}} = (8+1)^{2^{n-1}}$.

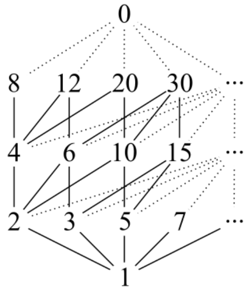
Por el Teorema del Binomio, tenemos

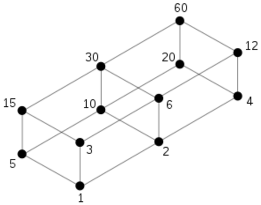
$$(x+y)^m = x^m + \binom{m}{1} x^{m-1}y + \binom{m}{2} x^{m-2}y^2 + \ldots + \binom{m}{m-1} xy^{m-1} + y^m.$$

En particular, para $x = 8$, $y = 1$ y $m = 2^{n-1}$, cada sumando de lado derecho de la ecuación anterior, excepto el último término $y^m = 1$, es un múltiplo de 8, en particular, múltiplo de 4. Luego $3^{2^n} = 4q + 1$, $q \in \mathbb{Z}$.

De ahí, el residuo de $3^{2^n} + 1 = 4q + 2$ y el residuo de $3^{2^n} + 1$ al dividirlo entre 4 es 2, lo que muestra que no es múltiplo de 4.

MDC y MMC





Dados $a, b \in \mathbb{Z}$, a cada uno les podemos asociar su conjunto de divisores no-negativos D_a y D_b respectivamente.

Por la propiedad de limitación, estos conjuntos son finitos, y su intersección $D_a \cap D_b$ es finita. Luego, $D_a \cap D_b$ posee un elemento máximo, llamado el *máximo divisor común* (MDC) de a y b.

De forma similar, los conjuntos de los M_a y M_b de múltiplos no-negativos de a y de b, respectivamente. Ahora $M_a \cap M_b$ es no vacío y limitado inferiormente por 0. Este conjunto posee un elemento mínimo, llamado el *mínimo múltiplo común* (MMC) de a y b.

Definición

Dados $a, b \in \mathbb{N}$, un ***máximo divisor común (MDC)*** *de a y b es un entero positivo d que satisface*

1. $d \mid a$ y $d \mid b$,
2. $k \mid d$, para todo $k \in \mathbb{N}$ tal que $k \mid a$ y $k \mid b$.

Similarmente, un ***mínimo múltiplo común (MMC)*** *de a y b es un entero positivo m que satisface*

1. $a \mid m$ y $b \mid m$,
2. $m \mid k$, para todo $k \in \mathbb{N}$ tal que $a \mid k$ y $b \mid k$.

De las definiciones anteriores, se sigue que el MDC y el MMC son únicos:

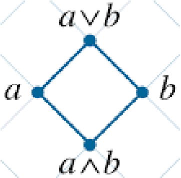
MDC y MMC

<u>Prueba</u>: Sean d_1 y d_2 dos MDC para a y b. Entonces $d_1 \mid a$, $d_1 \mid b$, $d_2 \mid a$, $2 \mid b$.
Como d_1 es MDC de a y b, y $d_2 \mid a$, $d_2 \mid b \;\Rightarrow\; d_1 \mid d_2$.
Como d_2 es MDC de a y b, y $d_1 \mid a$, $d_1 \mid b \;\Rightarrow\; d_2 \mid d_1$.
Entonces $|d_1| = |d_2|$, pero siendo d_1, d_2 no negativos, se concluye que $d_1 = d_2$.
La prueba es similar en el caso del MMC.

Notación. Como son únicos, denotamos por $d = (a, b)$ y por $m = [a, b]$ al MDC y MMC de a y b, respectivamente.

Otra forma de entender a $d = (a, b)$ y $m = [a, b]$ es que son el **ínfimo** y el **supremo**, respectivamente, de a y b, en la relación de divisibilidad $|$:

$$d = (a, b) = a \wedge b, \qquad m = [a, b] = a \vee b.$$



Ejemplo: Calcular el MDC y MMC de 360 y 84.
Solución: Factoramos los números 360 y 84 (en factores primos):

$$\begin{array}{r|l} 360 & 2 \\ 180 & 2 \\ 90 & 2 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \qquad\qquad \begin{array}{r|l} 84 & 2 \\ 42 & 2 \\ 21 & 3 \\ 7 & 7 \\ 1 & \\ & \\ & \end{array}$$

Los divisores coumnes para 360 y 84 son $2, 2, 3$. Entonces $(360, 84) = 2^2 \cdot 3 = 12$. Por otro lado, $[360, 84] = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$.

Propiedades (Propiedades MDC y MMC)

Sean $a, b, c \in \mathbb{N}$. *Entonces*

1. $(a, b) = a \;\Leftrightarrow\; [a, b] = b \;\Leftrightarrow\; a \mid b$.
2. $(ca, cb) = c(a, b)$ *y* $[ca, cb] = c[a, b]$.
3. $(a, b) = (b, a)$ *y* $[a, b] = [b, a]$.
4. $((a, b), c) = (a, (b, c))$ *y* $[[a, b], c] = [a, [b, c]]$.
5. $[(a, c), (b, c)] = ([a, b], c)$.
6. $([a, c], [b, c]) = [(a, b), c]$.
7. $(a, b)[a, b] = ab$.

Prueba: 1 a 6, Ejercicio!