DIVISIBILIDAD EN Z

Aunque la operación no es cerrada en $Z-\{0\}$, hay muchos ejemplos en donde un entero divide a otro, como por ejemplo:

2 divide a 6; 9 divide a 81. En este caso la división es exacta y no hay residuo (resto).

> Dados $a, b \in Z$ y $b \neq 0$.
>
> Se dice que b divide a a y se escribe $b|a$ si existe un elemento c tal que $a = b.c$.
>
> En este caso se dice que b es un divisor de a ó que a es un múltiplo de b.

Propiedades básicas: para $a, b, c \in Z$

1. $a \mid a$
   Esto es cierto dado que $a = 1.a$ ('|': resulta ser una relación reflexiva).

2. $1 \mid a$
   verdadero ya que $a = a.1$

3. $a \mid b \Rightarrow a \mid -b \wedge -a \mid b \wedge -a \mid -b$
   D/ Dado que H) $\exists k \in Z$: $b = a.\, k$; resultará:
   $b = (-a)\,(-k)$ de donde $-a \mid b$
   $-b = a\,(-k)$ de donde $a \mid -b$
   $-b = (-a)\,k$ de donde $-a \mid -b$

Consecuencia

Dado un número entero a: 1, -1, a, -a resultan ser divisores del mismo y son llamados <u>divisores triviales ó impropios.</u>

4. $a \mid 0$
   D/ $0 = 0.a$

5. $a \mid b \wedge b \mid c \Rightarrow a \mid c$
   D/ $a \mid b \wedge b \mid c \Leftrightarrow \exists k_1 \in Z$: $\underset{1}{b = k_1.a}$ $\exists\, k_2 \in Z$: $\underset{2}{c = k_2.b}$ (def '|')
   $\Rightarrow \exists k_3 \in Z$: $c = (k_2.\, k_1).a$ con $k_3 = k_2.\, k_1$ (1 en 2)
   $\Leftrightarrow a \mid c$ (def '|')

('|': resulta ser una relación transitiva)

6. $a \mid b \Rightarrow a \mid b.c$

D/ Por H) $\exists k \in Z$: $b = k.a$

Multiplicando ambos miembros por c: $b.c = \underbrace{(k.c)}_{k' \in Z}.a$

resulta entonces $a \mid b.c$

7. $a \mid b \wedge a \mid c \Rightarrow a \mid b + c$

D/ Por H) $\exists k_1, k_2 \in Z$: $(b = a.\, k_1 \wedge c = k_2\, .a)$

Entonces sumando miembro a miembro resulta: $b + c = \underbrace{(k_1 + k_2)}_{k_3 \in Z}.\, a$

De donde $a \mid b + c$

Un número entero positivo p $\neq$ 1 se dice **primo** si sus únicos divisores son los triviales, caso contrario se dice que es **compuesto**.
Así: 2, 3, 5, 7, ... son primos
4, 6, 8, 9, ... son compuestos.

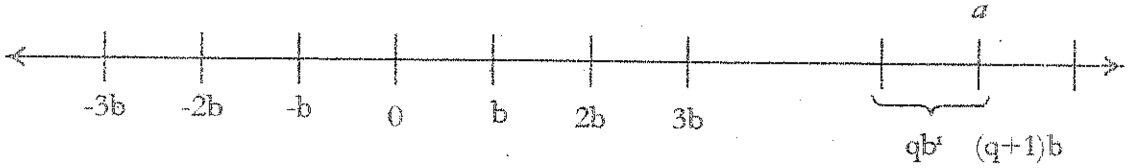
Algunas propiedades relativas:

- Si $m \in Z^+$ y m es compuesto, entonces existe un primo p tal que p | m.
- Hay infinitos números primos.

El algorítmo de la división:

Dados a, $b \in Z$ con $b > 0$ se trata de efectuar la división entera ó inexacta entre a y b. Es decir que se trata de aproximar "de la mejor manera posible" a a por un múltiplo de b. La diferencia entre a y dicho número es lo que llamamos el resto de la división; que será nulo en el caso en que a sea múltiplo de b.

Aclaremos esto:
Consideremos sobre la recta real los múltiplos de B.



Entonces el número representado por a debe caer en alguno de los intervalos que determinan dos múltiplos consecutivos de b.

Sea q $\in$ Z tal que $q.b \leq a < (q+1)b$

Y entonces de acuerdo a esto: $a = qb + r$ con $0 \leq r < b$
(b: amplitud del intervalo mencionado)

En definitiva se han determinado dos enteros q y r que se denominan respectivamente el cociente y el resto de la <u>división entera</u> de a por b verificando las condiciones;

$$\begin{cases} a = q.b + r & (1) \\ 0 \leq r < b & (2) \end{cases}$$

Las mismas caracterizan completamente al cociente y al resto. Dado que si se consideran (q_1, r_1) otro par de enteros que satisfacen dichas condiciones; es decir

$$\begin{cases} a = q_1.b + r_1 & (3) \\ 0 \leq r_1 < b \end{cases}$$

Haciendo (1)-(3) y considerando $q > q_1$ (el caso $q < q_1$ es similar)

Quedará $0 = (q - q_1).b + (r - r_1)$ sii $(q - q_1).b = r_1 - r$.
En consecuencia $r_1 - r > 0$ y además múltiplo de b y por otra parte $r_1 - r \leq r_1 < b$ lo que obviamente no es posible ($r_1 - r > b$ y $r_1 - r < b$).
Concluimos entonces que <u>$q = q_1$ y por ende $r_1 = r$</u>.

Observaciones:

1. De (1) y dividiendo por b resulta la igualdad.

$$\frac{a}{b} = q + \frac{r}{b}$$

y en (2) $\quad 0 \leq \frac{r}{b} < 1$

de donde
$$\begin{cases} q = \underbrace{\left[\frac{a}{b}\right]}_{\text{parte entera}} \text{ y } \boxed{a = \left[\frac{a}{b}\right].b + MANT\left(\frac{a}{b}\right).b} \\ \frac{r}{b} = \underbrace{MANT\left(\frac{a}{b}\right)}_{\text{MANTISA}} \end{cases}$$

✓ Así por ejemplo dados $a = 219$ y $b = 15$
La calculadora da 219: 15 = 14, 6
Así q = 14 y r = 0, 6. 15 = 9 ó r = 219 - 15. 14 = 9

✓ Y si se consideran $a = -219$ y $b = 15$

La calculadora da $-219: 15 = -14, 6$

Así $q = -15$ y $r = 0, 4. 15 = 6$ ó $r = -219 - 15. (-15) = 6$

2. El algoritmo de la división se puede generalizar de la siguiente manera:

Para $a, b \in Z$ y $b \neq 0$; existen $q, r \in Z$ únicos con $a = b. q + r$ y $0 \leq r < |b|$.
Si $b < 0$; efectuando la división entera de a y $-b$;
resultará por la anterior que $a = q' (-b) + r'$ con $0 \leq r' < -b$
ó bien $a = (-q').b + r'$
de donde $q = -q'$ y $r = r'$

Así por ejemplo:

✓ Si $a = 98$ y $b = -13$; como $= 98:13 \cong 7, 538$ — $q' = 7$, $r' = 7$

Resulta $q = -7$ y $r = 7$

✓ Si $a = -105$ y $b = -11$; como $-105: 11 \approx -9, 545$ — $q' = -10$, $r' = 5$

Resulta $q = 10$ y $r = 5$.

Máximo común divisor y mínimo común múltiplo.

Dados $a, b \in Z$ con al menos uno de ello distinto de cero, se denomina máximo común divisor de a y b a todo entero positivo d que satisface:

i) $d \mid a$ y $d \mid b$

ii) si $d' \in N$ y $d' \mid a$ y $d' \mid b$ entonces $d' \mid d$

El máximo común divisor de a y b existe y es único y se lo denota
(a, b)

Caso particular: si $a \mid b$, entonces $(a, b) = |a|$

Así por ejemplo $(-25, 50) = 25$; $(27, -18) = 9$; $(7, 0) = 7$

Si $(a, b) = 1$ se dice que a y b son <u>coprimos</u>.

Se denomina Mínimo común múltiplo de a y b a todo entero positivo m que satisface:

i) $a \mid m$ y $b \mid m$

ii) si $m' \in N$ satisface $a \mid m'$ y $b \mid m'$, entonces $m \mid m'$

El Mínimo común múltiplo de a y b existe y es único y se lo denota

$[a, b]$

"Se prueba" que:

$$\boxed{a.\ b = (a, b).\ [a, b]}$$

ALGORITMO DE EUCLIDES PARA HALLAR (a, b)

Dados los enteros a, b con $b \neq 0$; por el algoritmo de la división existen y son únicos q y $r \in Z$ tales que $a = b.\ q + r$ con $0 \leq r < |b|$.

1

Considerando $D(c, d) = \{x \in Z / x \mid c \text{ y } x \mid d\}$

Resultará $\underline{D(a, b) = D(b, r)}$

$D /\ x \in D(a, b) \Leftrightarrow x \mid a \wedge x \mid b$ (def. D (a; b)).

$\Rightarrow x \mid a \wedge x \mid b.\ q$ (propiedad de '|').

$\Rightarrow x \mid a\text{-}bq \wedge x \mid b$ (propiedad de '|').

$\Leftrightarrow x \mid r \wedge x \mid b$ (1).

$\Leftrightarrow x \in D(b, r)$

Con lo cual $\underline{D(a, b) \subset D(b, r)}$

En forma análoga $D(b, r) \subset D(a, b)$ (probarlo)

Y entonces repitiendo el proceso resultará:

$(a, b) = (b, r) = (r, r_1) = (r_1, r_2) = \ldots\ldots = (r_{n-1}, r_n)$ con $r_n = 0$.

$r_1 =$ resto $(b: r)$; $r_2 =$ resto $(r: r_1)$; $r_3 =$resto (r_1, r_2)…

$r_{n-1} =$ resto $(r_{n-3}: r_{n-2})$; $r_n =$ resto $(r_{n-2}: r_{n-1}) = 0$

De donde

$(a, b) = (r_{n-1}, r_n) = r_{n-1}$ con r_{n-1}: último resto no nulo de los sucesivos cocientes efectuados.

✓ Por ejemplo:

(614, 210) = (210, 194) = (194, 16) = (16, 2) = (2, 0) = 2

614 = 210. 2 + 194

210 = 194. 1 + 16

194 = 16. 12 + 2

16 = 2. 8 + 0

ó sea (614, 210) =2

Proposición:
Existen enteros s y t tales que (a, b) = s. a + t. b

✓ Por ejemplo: (2, 3) = 1 = 2. 2 + (-1). 3
o (2, 3) = 1= (-1). 2 + 1. 3
(15, 9) = 3 = (-1).15 + 2. 9

Observación: que d = s. a + t. b; no significa que d = (a, b)
Por ejemplo: 4 = 2. 2 + 0. 1 y 4 ≠ (2, 1)
Por otra parte si a | b; (a, b) = |a| = |a| + 0. B

Fuera de este caso trivial, se logra la expresión planteado por aplicación reiterada del algorítmo de Euclides. Lo veremos con ejemplos.
Se trata de hallar s y t tales que:

a) (515, 150) = s. 515 + t. 150

R/ a) 515 = 3. 150 + 65
150 = 2. 65 + 20
65 = 3. 20 + 5
20 = 4. 5
y entonces (515, 150) = 5 con
5 = 65 – 3. 20= 65 – 3. (150 – 2. 65)
= 7. 65 – 3. 150 = 7 (515 – 3. 150) – 3. 150
= (-24). 150 + (7). 515
de donde <u>s = 7 y t = -24</u>

b) (412, 224) = s. 412 +t. 224.

b) 412 = 224 + 188
224 + 188 + 36
188 = 5. 36 + 8
36 = 4.8 +4
8 = 4. 2
Así: (412, 224) = 4 = 36 – 4. 8
= 36 – 4 (188 – 5. 36) =
= 21. 36 – 4. 188 =
= 21 (224 – 188) – 4. 188 = 21. 224 – 25. 188
= 21. 224 – 25 (412 – 224)=
= 46. 224 – 25. 412
= (-25). 412 + (46). 224
de donde <u>s = -25 y t = 46</u>.

En particular si a y b son coprimos existen s, t: enteros tales que
1 = s. a + t. b

Propiedades relativas a los números primos y coprimos.

1. Si a, b; coprimos y $a\,|bc$ entonces $a \mid c$

D/ si a, b: coprimos; existen s y t $\in$ Z: 1 = sa +t. b.
Multiplicando por c: c = sa. c + t. b. c
Y entonces; por un lado como a | a; a| sac (1)
Y por hipótesis a | bc; de donde a | tbc (2)

De (1) y (2) por propiedad resulta a | sac + tbc sii a | c

2. Si p: primo y p | ab, entonces p | a p | b.
D/ si p | a nada hay que probar.
Si p X a; como p: primo; (a, p) = 1 y como existen extremos s y t tal que 1 = s.a +t. p

(si (a, p) = d $\neq$ 1; p no sería primo o p | a)

Multiplicando por b quedará: b = sa. b + t. p. b
y como por H) p | ab; p | sab y p | tpb; resultará que p | sab +tpb sii p | b.

Este resultado se gereraliza

si p: primo y p | $a_1.a_2....a_n$ $\left(p \mid \prod_{i=1}^{n} ai\right)$

Resultará que p | ai para algún i = 1, ... n.

Los números primos sirven como bloques de construcción para el conjunto de los enteros. Esto precisa el:

TEOREMA FUNDAMENTAL DE LA ARITMÉTICA.

Para cualquier m $\in$ Z^+, con n > 1; n es primo ó se puede escribir como un producto de primos, siendo esta representación única, salvo el orden (en este caso, se considera que un solo primo, es producto de un factor).

D/ Por absurdo

Suponiendo que existen enteros (> 1) que no son primos ni pueden representarse como producto de tales números; consideremos el menor de ellos: m. al no ser primo, admite un divisor p $\neq$ 1, m tal que m = p. k con 1 < p, k < m. pero esto significa que p y k son factorizables en producto de primos; pero entonces contra lo supuesto m también lo es. Absurdo. Resta probar la unicidad de la descomposición.

Sean dos descomposiciones de m en factores primos:

(1)

$m = q_1 . q_2 . \ldots . q_s = r_1 . r_2 . \ldots . r_l$ con $q_i, r_j > 1$

Entonces $q_1 \mid r_1 . r_2 \ldots r_l$ y por propiedad anterior q_1 divide por lo menos a un factor r_j; pero como q_1 y r_j son primos, resulta $q_1 = r_j$ entonces ordenando el producto en (1) para que aparezca r_j al comienzo y simplificando q_1 con r_j quedará:

$$q_2 . q_3 \ldots q_s = \underbrace{r'_2 . r'_3 \ldots r'_l}_{\text{nuevo orden de } r_j}$$

Repitiendo el proceso de simplificación, cada factor de la primera descomposición se simplificará con algún factor de la segunda descomposición siendo $s \leq l$. En forma análoga partiendo de que cada r_j divide a algún q_i resultará que $l \leq s$ de donde $s = l$ y la descomposición es única.

Observación: En una descomposición puede aparecer un número primo p varias veces. Entonces agrupando los factores idénticos podrá escribirse:

$$n = p_1^{l_1} . p_2^{l_2} \ldots p_k^{l_k} \quad \text{con } 1 < p_1 < p_2 < \ldots < p_k$$

Consecuencia:

Si m, n $\in Z^+$ tal que $\begin{cases} m = p_1^{e} . p_2^{e} \ldots p_k^{e} . p_{k+1}^{e} \ldots p_l^{e} \\ n = p_1^{f_1} . p_2^{f_2} \ldots q_k^{f_k} . q_{k+1}^{e_{k+1}} \ldots q_s^{f_s} \end{cases}$

(descomposiciones de m y n en factores primos)

Sí $a_i = \min \{e_i, f_i\}$; se obtiene

$$(m, n) = \prod_{i=1}^{n} p_i^{a_i}$$

¿Cómo se obtendría [m, n]?

CONGRUENCIA MÓDULO N
(una relación de equivalencia definida en Z)

Dados los enteros a, b y n, se dice que a *es congruente con b módulo n* y se escribe $a \equiv b(n)$ sii $n / a-b$ o sea $\exists\, k \in Z : a-b = k.n$
Por ejemplo: $4 \equiv 10\ (3)$ pues $4-10 = (-2).3$
La relación de congruencia módulo n es una relación de equivalencia. Vamos a probarlo:

Reflexividad $\forall a \in Z : n / a-a$ *pues* $a-a = 0.n$ *de donde* $a \equiv a\ (n)$

Simetría

$$\forall a \in Z\ \forall b \in Z : a \equiv b(n) \Leftrightarrow \exists\, k \in Z : a-b = k.n$$
$$b-a = -k.n$$
$$b-a = h.n \qquad h = -k$$
$$\Leftrightarrow b \equiv a(n)$$

Transitividad:

$$\forall a \in Z\ \forall b \in Z : \forall c \in Z :\ a \equiv b(n) \wedge b \equiv c(n) \Leftrightarrow$$
$$\exists\, k_1 \in Z : a-b = k_1\, n \ \wedge\ \exists\, k_2 \in Z : b-c = k_2 .n$$
$$\Rightarrow a-c = (k_1+k_2).n \quad \textit{siendo} \quad k_1+k_2 = k \in Z$$
$$\Leftrightarrow a \equiv c(n)$$

Por ser la congruencia una relación de equivalencia, determina una partición del conjunto de los enteros en clases de equivalencia que se denominan *clases de congruencia módulo n.* Dos números enteros pertenecen a la misma clase sii son congruentes módulo n.
Vamos a determinar las clases de equivalencia y el conjunto cociente.
Sea $a \in Z$ entonces $cl_a = \{x : x \in Z \wedge x \equiv a(n)\}$

$$x \equiv a(n) \ \ sii \ \ x-a = kn$$
$$x = a + k.n \quad k \in Z$$

es decir, a la clase del a pertenecen las sumas de a con todos los múltiplos de n.
En particular:

$K_0 = cl(0) = cl_0 = \{........., -2n. -n,\ 0,\ n,\ 2n, 3n, ...\}$
$K_1 = cl(1) = cl_1 = \{..........., 1-2n,\ 1-n,\ 1,\ 1+n,\ 1+2n,\ 1+3n, ...\}$
$K_2 = cl(2) = cl_2 = \{............, 2-2n,\ \ 2-n,\ 2,\ \ 2+n,\ \ 2+2n, ...\}$
....
$K_{n-1} = cl(n-1) = cl_{n-1} = \{................, -1-2n,\ -1-n;\ \ -1.,\ \ -1+n,\ \ -1+2n, ...\}$

Si consideramos K_n va a coincidir con K_0

8a

Los subíndices de las clases de equivalencia son los posibles restos de la división de un entero por n, es decir: $0, 1, 2 \ldots\ldots, n-1$ ya que de acuerdo con el algoritmo de la división entera el resto es no negativo y menor que el módulo del divisor. Por ello, reciben el nombre de *clases de restos módulo n* y se los indica $\overline{0}$, $\overline{1}$, $\overline{2}$, ,,,,,, $\overline{n-1}$

El conjunto cociente es $\dfrac{Z}{\equiv_{(n)}} = \left\{ \overline{0}, \overline{1}, \overline{2}, \ldots\ldots, \overline{n-1} \right\} = Z_n$

$Z_n = \{ R_{i} / 0 \leq i < n \}$

Probaramos en clase que es una partición de Z!