Edgard A. Araya C.
Álgebra I - Ay. 09
29/Julio/2019

Divisibilidad y Algoritmo de la División

1. Determine cuociente y resto para las divisiones enteras siguientes:

   (A) $a = 2345$, $b = 12$
   (B) $a = 123456$, $b = 23$
   (C) $2335 = a$, $b = 22$
   (D) $a = -2335$, $b = 22$
   (E) $a = -2335$, $b = -22$.

2. Dados $a, b, c \in \mathbb{Z}$, demostrar las propiedades:

   (A) $a \mid a$
   (B) $a \mid ab$
   (C) $a \mid b \wedge b \mid c \Longrightarrow a \mid c$
   (D) $a \mid b \wedge b \mid a \Longrightarrow a = \pm b$
   (E) $a \mid b \wedge a \mid c \Rightarrow a \mid mb + nc$ $(m, n \in \mathbb{Z})$
   (F) $a \mid (b+c) \wedge a \mid b \Rightarrow a \mid c$
   (G) $a \mid b \wedge a \mid c \Longrightarrow a \mid b+c$

3. Sea $n = a^2$, $a \in \mathbb{N}$ (es decir, n es cuadrado perfecto). Demostrar que al dividir n por 4, se obtiene resto 0 ó 1.

4. Demostrar que para $a, b \in \mathbb{Z}^+$ se cumple:

   $$MCD(a, b) = d \Longrightarrow MCD\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

5. Sean $a, b, c \in \mathbb{Z}^+$. Demostrar que:

   (A) Si a y b son primos relativos, entonces b y $(a + bc)$ son primos relativos.

   (B) Si a y c son primos relativos y b y c son primos relativos, entonces ab y c son primos relativos.

6. (A) Determinar $MCD(120, 84)$.
   (B) Determinar $MCD(80, 651)$.
   (C) Determinar $MCD(1066, 1492)$.

7. Determine, para los valores de a, b y $d = MCD(a, b)$ en cada uno de los ejercicios de la parte (6), los valores de $m, v \in \mathbb{Z}$ tales que $\boxed{d = (m) \cdot a + (v) \cdot b}$ (Bezout)

Algoritmo de la División

* Versión Preliminar (divisor positivo)

Si $a, b \in \mathbb{Z}$, con $b > 0$, existen únicos $q, r \in \mathbb{Z}$ tales que

$$\boxed{a = (q)\cdot b + (r)} \quad \wedge \quad \boxed{0 \leq r < b}$$

Casos: * $\boxed{a = 9,\ b = 4} \Longrightarrow 9 = (2)\cdot 4 + (1) \ \wedge \ 0 \leq 1 \leq 4$

$\Longrightarrow \boxed{q = 2,\ r = 1}$

* $\boxed{a = -9,\ b = 4} \Longrightarrow -9 = (-3)\cdot 4 + (3) \ \wedge \ 0 \leq 3 < 4$

$\Longrightarrow \boxed{q = -3,\ r = 3}$

$(b<0)$ ¡OJO!

* $\boxed{a = 9,\ b = -4} \Longrightarrow 9 = (-2)(-4) + 1 \ \wedge \ 0 \leq 1 < -4$

¿Cómo agregar a los divisores negativos?

* Versión Completa (divisor cualquiera, excepto cero).

Si $a, b \in \mathbb{Z}$, con $b \neq 0$, existen únicos $q, r \in \mathbb{Z}$ tales que

$$\boxed{a = (q)\cdot b + (r)} \quad \wedge \quad \boxed{0 \leq r < |b|}$$

Divisibilidad en $\mathbb{Z}$

Def: * Sean $a, b \in \mathbb{Z}$ tal que $a = (q)b$ para algún $q \in \mathbb{Z}$. En tal caso, escribiremos $a | b$. En caso contrario, se escribirá $a \nmid b$.

* Nombres para "$a|b$":
  * a es divisible por b.
  * a es múltiplo de b.
  * b es factor de a.
  * b es divisor de a.
  * b divide a a.

Obs: Debido al Algoritmo de la División, los divisores de un número pueden ser positivos y negativos!!!

Máximo Común Divisor (MCD)

<u>Def:</u> Se dice que $d \in \mathbb{Z}$ es el <u>máximo común divisor</u> entre $a \in \mathbb{Z}$ y $b \in \mathbb{Z}$ ($d = MCD(a,b) = (a,b)$) si se cumple:

(i) $d \mid a \wedge d \mid b$

(ii) Si $c \in \mathbb{Z}$ es tal que $c \mid a \wedge c \mid b$, entonces $c \mid d$.

<u>Def:</u> Si a y b son tales que $MCD(a,b) = 1$, se dice que a y b son primos relativos (coprimos).

Algoritmo de Euclides

<u>Teorema:</u> Si $a = (q)b + (r)$, entonces $MCD(a,b) = MCD(b,r)$

<u>Teorema:</u> El último resto no nulo en el Algoritmo de Euclides corresponde al máximo común divisor buscado.

Identidad de Bezout

Si $a, b \in \mathbb{Z}$ no ambos nulos, entonces existen $u, v \in \mathbb{Z}$ tales que $MCD(a,b) = (u)\cdot a + (v)\cdot b$