CAP. 5 NÚMEROS ENTEROS

Algoritmo de la división.

Principio del buen orden Todo conjunto no vacío de enteros positivos posee un menor elemento.

El principio del buen orden nos garantiza que cualquier subconjunto del conjunto de los números enteros que contiene sólo números positivos, contiene un entero positivo menor que todos los demás.

Por ejemplo, el conjunto de los enteros positivos pares tiene un menor elemento, el 2.

Teorema (El algoritmo de la división) Dados dos enteros cualesquiera a y b con $b>0$, existen únicos enteros q y r tales que

$$\boxed{a = qb + r} \quad y \quad \underline{0 \le r < b}$$

Dem. Considere la progresión aritmética

$$\ldots, a-3b, a-2b, a-b, a, a+b, a+2b, a+3b, \ldots$$

En esta sucesión elegimos el menor número no negativo y lo denotamos por r. Por tanto, por definición, r satisface la desigualdad del teorema pero también r, estando en la sucesión, es de la forma $a-qb$ y así q está definido en término de r.

Es decir $\quad r = a - qb \Rightarrow \underline{a = qb + r}$, además $0 \le \underline{a-qb < b}$

$0 \le r$, $\quad \underline{a-qb} > b \quad$ pero $q\cancel{b}+r > q\cancel{b}+b$

$a > qb + b \qquad \underline{r > b}$

Por ejemplo sean $a = 72$ y $b = 15$, entonces

$72-75,\ 72-60,\ 72-45,\ 72-30,\ 72-15,\ 72,\ 72+15,\ 72+30,\ 72+45, \dots$

$-3,\ 12,\ 27,\ 42,\ 57,\ 72,\ 87,\ 102,\ 117.$

Así $r = 12$ con $0 < 12 < 15$

además $r = 12 = 72 - 4 \cdot 15$

o $72 = 4 \cdot 15 + 12$

$a = q \cdot b + r$

Ej. Ilustre el algoritmo de la división, encontrando q y r para cada par a y b.

1. $a = 132$, $b = 7$
2. $a = -52$, $b = 3$
3. $a = 541$, $b = 16$
4. $a = 36$, $b = 5$

Sol.

1. Si $a = 132$, $b = 7$

$a = q \cdot b + r$

$132 = 18 \cdot 7 + 6$

$$\begin{array}{r|l} 132 & 7 \\ \hline 62 & 18 \\ (6) & \end{array}$$

Así $q = 18$ y $\boxed{r = 6}$

2. Si $a = -52$, $b = 3$

$-52 = (-18) \cdot 3 + 2$

Así $q = -18$ y $\boxed{r = 2}$

3. Si $a = 541$, $b = 16$

$541 = (33) \cdot 16 + (13)$

Así $q = 33$ y $\boxed{r = 13}$

4. Si $a = 36$, $b = 5$

$36 = (7) \cdot 5 + 1$

$q = 7$, $\boxed{r = 1}$

Ejm. Si $a = -14$ y $b = 3$

$-14 = (-4)3 - 2$, $\underline{-2} < 3$, $0 \not\leq -2$

$-14 = (-5) \cdot 3 + 1$ $0 \leq 1 < 3$

Corolario Sean a y c enteros con $c \neq 0$, entonces existen únicos enteros q y r tal que $a = q \cdot c + r$, $0 \leq r < |c|$

Por ejm. $a = 37$ y $c = -5$

$$37 = (-7)(-5) + 2 \quad , \quad 0 \leq 2 \leq |-7| = 7$$

Divisibilidad

Def. Un entero b es divisible por un entero a, $a \neq 0$, si existe un entero x tal que $b = ax$ y se escribe $a|b$.

Si b no es divisible por a, escribimos $a \nmid b$.

La expresión $a|b$ significa que <u>a divide a b</u>, o que <u>a es divisor de b</u> o que <u>b es multiplo de a</u>, o <u>b es divisible por a</u>.

Si $a|b$ y $0 < \underline{a < b}$, entonces a es un divisor propio de b.

Así nunca se tendrá $0|b$, pero $a|0$ es siempre verdad, $a \neq 0$

Ejm. $3|24$ porque $24 = 3 \cdot (8) + 0$, $0 < 3 < 24$

$3 \nmid 17$ porque $17 = 3(?)$,

$-6|54$ porque $54 = (-6) \cdot (-9) + 0$

$-6 \nmid -13$ porque $-13 = (-6)(?)$

Ejm. $a|0$ porque $0 = a \cdot 0$

Obs. Si $a|b$ es decir $b = a \cdot c$, entonces $(-b) = a(-c)$

Así $a|-b$, $\therefore$ b y $-b$ tienen los mismos divisores.

Def. a) El entero a es un divisor común de b y c en el caso de que

$a|b$ y $a|c$

puesto que existe un número finito de divisores de cualquier entero diferente de cero, solamente existe un número finito de divisores comunes de b y c, excepto si $a=b=0$.

div $8=\{1,2,4,8\}$ ✓

div. $30=\{1,2,3,5,6,10,15,30\}$ ✓

div. $0=\{1,2,3,4,\ldots\}$

Def. (máximo común divisor) Sean a y b enteros no ambos 0. El máximo común divisor de a y b, es el entero mas grande d que divide a a y b. En otras palabras si d es el máximo común divisor de a y b entonces

i) $d|a$ y $d|b$ i) $\underline{6}|30 \wedge \underline{6}|12$

ii) Si $\underline{c}|a$ y $c|b$ entonces $c|d$ ii) $2|30 \wedge 2|12 \Rightarrow \underline{\underline{2|6}}$

El máximo común divisor de a y b, se denota por (a,b)

Si a y b no son ambos cero, el máximo común divisor existe y es único. Esto porque enteros no ceros tienen un número finito de divisores y así se tiene sólo un número finito de divisores comunes y el mayor de ellos será el máximo común divisor. Por lo tanto

$$(a,b)\geq 1 \quad , \text{ porque 1 es comun div. de } a \text{ y } b.$$

Ejm. a) $(12,30)=6$

div. $12=\{\pm1,\pm2,\pm3,\pm4,\pm6\ \pm12\}$

div. $30=\{\pm1,\pm2\ \pm3\ \pm5\ \pm6\ \pm10\ \pm15\ \pm30\}$

div. comunes $= \{\pm 1, \pm 2, \pm 3, \pm 6\}$

máximo común divisor $= \{6\}$ $\Rightarrow (12,30) = 6$

b) $(10,21) = 1$ div. $20 = \{1,2,4,5,10,20\}$

$a \neq 1$

c) $(a,0) = a$ div. $0 = \{1, 2, \ldots, 20, 21, \ldots\}$

div com. $= \{1,2,4,5,10,20\}$

Dos numeros cuyo $(a,b) = 1$, se llaman primos relativos

Números primos Un número $p > 0$ se llama primo si tiene sólo 2 divisores $\{1, p\}$

Si un número tiene 3 o más divisores se llama compuesto.

Teorema. Todo número compuesto tiene un factor primo.

Dem. Sea n un número compuesto, entonces

$$n = n_1 \cdot n_2 \quad , \quad n_1 \neq 1 \quad , \quad n_2 \neq 1$$

Si n_1 y n_2 son números primos, queda demostrado teorema. Pero si $\underline{n_1}$ no es primo y $\underline{n_2 \text{ es primo}}$ entonces

$$\underline{n_1 = n_3 \cdot n_4} \quad , \quad \text{Así} \quad n = \underline{n_3 \cdot n_4 \cdot n_2}$$

Si n_3 y n_4 son primos entonces se tiene el teorema

Pero si $\underline{n_3}$ no es primo y $\underline{n_4}$ es primo, entonces

$$n_3 = n_5 \cdot n_6 \quad \Rightarrow \quad n = \underline{n_5 \cdot n_6 \cdot n_4 \cdot n_2}$$

Así $n > n_1 > n_3 > n_5 > \cdots > n_{2k-1} > 0$

y el proceso continua hasta obtener un factor primo.

Por tanto todo numero compuesto posee un factor primo.

Método para determinar

Crit. de divisibilidad

2: $20243 8\boxed{}$

0, 2, 4, 6, 8.

3: abcd

$a+b+c+d = 3\cdot\boxed{}$

$6 = 3\cdot 2$

4: $abcdef\boxed{}$

1 32

5: $abcdef\boxed{0}$

5

6: abcdef div 2, div 3

7: