PRACTICO 1

Teorema de División Entera

Dados $a, b \in \mathbb{Z}$, $b \neq 0$, $\exists! q, r \in \mathbb{Z}$ con $0 \leq r < |b|$ t.q $a = b.q + r$

Consecuencia

$\forall a, b \in \mathbb{Z}$, $b > 0$. $\exists! a_0, a_1, \dots, a_n \in \mathbb{N}$ con $0 \leq a_i < b$ t.q $a = a_n.b^n + \dots + a_1.b + a_0$

En donde los a_i son los coeficientes de a en base b. $a = (a_n \dots a_1 a_0)_b$

Notación: Si $m|n$ decimos que m es un divisor de n

- $Div(n) = \{ m \in \mathbb{Z} : m|n \}$
- $Div_+(n) = \{ m \in \mathbb{N} : m|n \}$

OBS: 1) $Div(0) = \{ m \in \mathbb{Z} : m|0 \} = \{ m \in \mathbb{Z} : \exists c \in \mathbb{Z} : 0 = m.c \} = \mathbb{Z}$

2) Si $n \neq 0$ $Div(n) \subseteq \{ \pm 1, \pm 2, \dots, \pm n \}$

Definición: $p \in \mathbb{N}$ es un numero primo si $\#Div_+(p) = 2$

Obs: 1) $p = 1$ no es primo $\#Div(p) = 1$

2) Si $p \neq 1$, p es primo $\iff Div_+(p) = \{1, p\}$

Maximo Comun Divisor

Sean $a, b \in \mathbb{Z}$, definimos el $m(a,b)$ como:

$mcd(a,b) = \max(Div(a) \cap Div(b)) = \max \{ x \in \mathbb{Z} : x|a \text{ y } x|b \}$

Propiedades:

1) $mcd(1,a) = 1$ $\forall a \in \mathbb{Z}$
2) $mcd(a,b) = |b|$ $\forall b \in \mathbb{Z}$
3) $mcd(a,b) = mcd(|a|,|b|)$ $\forall a, b \in \mathbb{Z}$

Proposición: Sean $a, b \in \mathbb{Z}$ con $a, b \neq 0$ entonces:

1) $mcd(a,b) = mcd(b, a - bx)$
2) En particular si r es el resto de dividir a entre b $\Rightarrow mcd(a,b) = mcd(b,r)$

Definición: Si $m, n \in \mathbb{Z}$ decimos que m divide a n si $\exists c \in \mathbb{Z}$ t.q $n = m.c$

Notación: $m|n$

Propiedades

1) Si $m \neq 0 \Rightarrow m|n \iff resto(n,m) = 0$
2) $\pm 1 | n$ $\forall n \in \mathbb{Z}$, $n = 1.n$, $n = (-1)(-n)$
3) $m|0$ $\forall m \in \mathbb{Z}$, $0 = m.0$
4) $0|0$ ya que $0 = 0.c$ $\forall c \in \mathbb{Z}$
5) Si $m|n$ y $n \neq 0$, $|m| \leq |n|$
   $n = m.c \Rightarrow |n| = |mc| = |m|.|c| \geq |m|$
   $n \neq 0 \Rightarrow c \neq 0 \Rightarrow |c| \geq 1$
6) Si $m|n$ y $m|p \Rightarrow \forall x, y \in \mathbb{Z}$ $m | nx + py$ siendo esta una combinación lineal entera
7) Si $m|n$ y $m|p$, $p \neq 0$ $\Rightarrow m | resto(n,p)$ Si $n = p.q + r$ $\Rightarrow m|r$
8) Si $dm|dn$ y $d \neq 0 \Rightarrow m|n$ $\forall d \in \mathbb{Z}$
9) Si $m|n \Rightarrow dm|dn$ $\forall d \in \mathbb{Z}$

+ Propiedades Practico

- Si $a|b$ y $c|d \Rightarrow ac | b.d$
- Si $a | bc \Rightarrow a|b$ y $a|c$
- Si $4 | a^2 \Rightarrow 2|a$

+ Propiedades Practico (mcd)

- $mcd(ca, cb) = c.mcd(a,b)$
- Si $c|a$ y $c|b$ entonces $mcd(a/c, b/c) = mcd(a,b)/c$
- $mcd(b, a+bc) = mcd(a,b)$
- Si a es par y b impar $\Rightarrow mcd(a,b) = mcd(a/2, b)$
- $mcd(a,b) = mcd(a-b, b)$
- $(a,b) = 1 \Rightarrow mcd(a-b, a+b) = 1$ o 2