Teorema (9.9.5)

[Algoritmo de la división]- Si $a, b \in \mathbb{Z}$ y $b \neq 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tales que:

$$a = bq + r \quad y \quad 0 \leq r < |b|$$

Demostración:

Supongamos primero que $b > 0$. En tal caso $|b| = b$. Sea:

$$A = \{a - bx \mid x \in \mathbb{Z} \text{ y } a - bx \geq 0\}$$

Claro que $A \subset \mathbb{N} \cup \{0\}$, y puesto que no hay enteros entre 0 y 1, entonces $\mathbb{N} \cup \{0\}$ está bien ordenado por $\leq$.

Veamos que $A \neq \emptyset$: Como $b > 0$, entonces $b \geq 1$, por tanto:

$$-b \leq -1$$

entonces:

$$-b|a| \leq -|a|$$

y como $-|a| \leq a$, entonces:

$$-b|a| \leq a$$

por tanto:

$$a - b(-|a|) \geq 0$$

tomando $x = -|a|$ se cumple que $a - bx \in A$.

Como $\mathbb{N} \cup \{0\}$ está bien ordenado, entonces A tiene elemento mínimo, digamos que este es r. Entonces:

$$r = \min A$$

Como $r \in A$, entonces $\exists\, q \in \mathbb{Z}$ tal que:

$$r = a - bq$$

por tanto:

$$a = bq + r \quad y \quad 0 \leq r$$

afirmamos que $r < b = |b|$.

Si $b \leq r$, entonces:

$$0 \leq r - b < r$$

$0 < b \Rightarrow -b < 0$

$\Rightarrow r - b < r + 0$

Nota: 0 y 1

Suponga que $c = \min D^+$, $c < 1$.

luego $c \in D^+ \Leftrightarrow 0 < c \Rightarrow 0 < c < 1$

$\Rightarrow 0 < c^2 < c < 1 \Rightarrow c^2 = \min D^+ \#_c$

pues $c^2 \neq c = \min D^+$. Así, 1 es el mínimo de D^+.

y como $r = a - bq$, entonces:

$$r - b = a - bq - b$$
$$\Rightarrow r - b = a - b(q+1)$$
$$\Rightarrow r - b = a - b(q+1) \in A$$

y:

$$r - b < r$$

lo cual es una contradicción, pues $r = \min A$. Por tanto:

$$0 \leq r < b = |b|$$

Supongamos que $b < 0$, entonces $0 < -b$. Por lo probado anteriormente, existen q', $r' \in \mathbb{Z}$ tales que:

$$a = (-b)q + r', \text{ con } 0 \leq r' < -b = |b|$$

por tanto:

$$a = b(-q') + r', \text{ con } 0 < r' \leq |b|$$

entonces existen $q, r \in \mathbb{Z}$, $q = -q'$, $r = r'$ tales que:

$$a = bq + r, \text{ con } 0 \leq r < |b|$$

probaremos la unicidad de q y $r \in \mathbb{Z}$.

Supongamos que:

$$a = bq + r \text{ y } 0 \leq r < |b|$$

y:

$$a = bq' + r' \text{ y } 0 \leq r' < |b|$$

entonces:

$$bq + r = bq' + r' \text{ y } 0 \leq r < |b| \text{ y } 0 \leq r' < |b|$$
$$\Rightarrow r - r' = b(q' - q) \text{ y } 0 \leq r < |b| \text{ y } 0 \leq r' < |b|$$

por tanto, $b \mid r - r'$, entonces $r - r' = 0$ o $|b| \leq |r - r'|$.

Pero esto último no puede ocurrir, pues:

$$0 \leq r < |b| \text{ y } 0 \leq r' < |b|$$

por tanto:

$$-|b| < r - r' < |b|$$
$$\Rightarrow |r - r'| < |b|$$

En consecuencia: $r-r'=0 \Rightarrow r=r' \Rightarrow q=q'$.

q.e.d.

Definición (4.4.6):

Sean $a, b \in \mathbb{Z}$, no ambos cero. Decimos que $d \in \mathbb{Z}, d>0$ es un máximo común divisor (mcd) de a y b, si:

i) $d|a$ y $d|b$.

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

Notación: Para decir que d es mcd de a y b, escribiremos $d=(a,b)$ ó $d=mcd\{a, b\}$.

Proposición (4.4.7)

Ver las proposiciones y lemas.

Si $d=(a,b)$, entonces d es único.

Teorema (4.4.10):

Si $a,b \in \mathbb{Z}$ son no ambos cero, entonces existe $d \in \mathbb{Z}$ tales que:

$$d=(a,b)$$

Además, d es el mínimo entero positivo para el cual existen $s,t \in \mathbb{Z}$ tales que:

$$d=as+bt.$$

Dem:

Sea:

$$A=\{ax+by \mid x,y \in \mathbb{Z} \text{ y } ax+by>0\}$$

entonces $A \subset \mathbb{N}$. Además $A \neq \emptyset$, pues eligiendo $x=a$ y $y=b$:

$$ax+by=a\cdot a+b\cdot b=a^2+b^2>0+0=0$$

por tanto, $a^2+b^2 \in A$.

Como $\mathbb{N}$ está bien ordenado, entonces tiene elemento mínimo. Sea:

$$d=\min A$$

entonces $\exists\ s,t \in \mathbb{Z}$ tales que:

$$d=as+bt.$$

Probaremos que $d=(a,b)$.

Claro que $d>0$.

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

Por algoritmo de la división, existen q, r tales que:

$$a = dq + r \quad y \quad 0 \leq r < d$$

Como $d = as + bt$, entonces:

$$a = (as+bt)q + r \quad y \quad 0 \leq r < d$$

por tanto:

$$r = a(1-sq) - b(tq) \quad y \quad 0 \leq r < d$$

entonces $r \in A$ y por tanto $0 \not< r$ y $r \not< d$, $d = min A$. Por tanto: $r = 0$.

y como:

$$a = dq + r$$

entonces $d \mid a$.

análogamente, $d \mid b$.

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

como:

$$d = as + bt$$

y $c \mid a$ y $c \mid b$, entonces $c \mid d$.

q.e.d.

obs: si $1 = as + bt$, entonces: $(a, b) = 1$.

Proposición (4.4.11)

Si $a, b \in \mathbb{Z}$ son no ambos cero, entonces:

$$(a, b) = (|a|, |b|)$$

Definición (4.4.12)

Sea $n \in \mathbb{N}$, y sean:

$$a_0, \ldots, a_n \in \mathbb{Z}$$

no todos cero. Decimos que $d \in \mathbb{Z}$ es mcd de $a_0, \ldots, a_n$, si $d > 0$ y:

i) $d \mid a_k \ \forall k = 0, 1, \ldots, n$.

ii) Si $c \in \mathbb{Z}$ es tal que $c \mid a_k$ $\forall$ $k = 0, \dots, n$, entonces $c \mid d$.

Notación: para decir que d es mcd de $a_0, \dots, a_n$, escribiremos:

$$d = (a_0, a_1, \dots, a_n)$$

$$d = \text{mcd}\{a_0, a_1, \dots, a_n\}$$

Proposición (9.9.13)

Definición (9.9.17)

Decimos que $p \in \mathbb{Z}$ es número primo, si $p > 1$ y los únicos divisores positivos de p, son 1 y p mismo.

Teorema (9.4.18)

Sean $a, b, a_1, \ldots, a_n \in \mathbb{Z}$ y sea p un número primo. Entonces:

i) $p \nmid a \Leftrightarrow (a, p) = 1$.

ii) $p \mid ab \Rightarrow p \mid a$ o $p \mid b$.

iii) $p \mid a_1 \cdot \ldots \cdot a_n \Rightarrow p \mid a_i$ para algún $i = 1, 2, \ldots, n$.