Teoría de números Verano 2018*

Oromion
Facultad de Ciencias – Universidad Nacional de Ingeniería

Actualizado a la fecha 12 de enero del 2018

*Grupo Estudiantil de Matemática y al Instituto de Matemática y Ciencias Afines

Capítulo 1

Introducción

I. *Principio de inducción matemática*

Sea $\mathcal{P}$ un conjunto de números naturales tal que

a) $1 \in \mathcal{P}$.

b) Si $n \in \mathcal{P} \implies n+1 \in \mathcal{P}$.

$\therefore \boxed{\mathcal{P} = \mathbb{N}}$.

II. *Principio del buen orden*

Si $\mathcal{A}$ es un conjunto no vacío de $\mathbb{N}$, entonces $\mathcal{A}$ *posee un elemento mínimo*.

1.1. Divisibilidad

Definición 1.1. *Sean d y n dos números enteros, se denotará*

$$\boxed{d \text{ divide a } n \iff \text{existe } c \in \mathbb{Z} \text{ tal que } n = c \cdot n}$$

como $a \mid n$.
Si d no divide a n, es decir, si $\forall c \in \mathbb{Z}\colon n \neq c \cdot d$, se denotará como $d \nmid n$.

1.2. Propiedades de la operación $|$

1) $n \mid n$ para cualquier $n \in \mathbb{N}$ (Reflexividad).

2) Si $d \mid n$ y $n \mid m$, entonces $d \mid m$. (Transitividad).

3) Si $d \mid n$ y $d \mid m$, entonces $d \mid an + bm \ \forall a, b \in \mathbb{Z}$.

4) Si $d \mid n$, entonces $ad \mid an$.

5) Si $ad \mid an$ con $a \neq 0$, entonces $d \mid n$.

6) $1 \mid n$ para cualquier $n \in \mathbb{N}$.

7) $n \mid 0$ para cualquier $n \in \mathbb{N}$.

8) Si $0 \mid n$, entonces $n = 0$.

9) Si $d \mid n$ y $n \neq 0$, entonces $|d| \leqslant |n|$.

10) Si $d \mid n$ y $n \mid d$, entonces $|d| = |n|$.

11) Si $d \mid n$ con $d \neq 0$, entonces $\left(\frac{n}{d}\right) \mid n$.

1.3. Máximo común divisor

Definición 1.2. *Sean a, b y d números enteros. Si $d \mid a$ y $d \mid b$, entonces d es un divisor común de a y b.*

Teorema 1.1. *Dados los números enteros a y b, existe un divisor común d de a y b de la forma $d = ax + by$ para cualesquiera $x, y \in \mathbb{Z}$.*

Prueba: Por inducción matemática en $K = |a| + |b|$.

Si $K = 0$, entonces $a = b = 0$, esto es, $d = 0 \cdot a + 0 \cdot b$. ✓

Supongamos que se cumple para $K = 0, 1, \ldots, n - 1$. (Hipótesis de inducción matemática).

Demostraremos para $\boxed{K = n = |a| + |b|}$.

Sin pérdida de generalidad, suponga que $|a| \geqslant |b|$. Así, si $|b| = 0$, entonces $b = 0$ y $|a| = n \implies d = n = (1)(\pm 1) + 0 \cdot b$.

Si $|b| \geqslant 1$, entonces para los números $|a| - |b|$ y $|b|$ se cumple la hipótesis:

$$\underbrace{|a| - |b|}_{\geqslant 0} + |b| = |a| - \cancel{|b|} + \cancel{|b|} = |a| < |a| + |b| = n.$$

Existe $d \in \mathbb{Z}$, $d \mid |a| - |b|$ y $d \mid |b|$. Además:

$$\begin{aligned}
d &= (|a| - |b|)\, x' + |b| y' \qquad\qquad \forall x', y' \in \mathbb{Z} \\
d &= |a| \underbrace{x'}_{x''} + |b| \underbrace{y'}_{y''} \\
d &= \underbrace{|a|}_{a,-a} x'' + \underbrace{|b|}_{b,-b} y'' \\
d &= a \underbrace{x''}_{\pm x'} + b \underbrace{y''}_{\pm y'}
\end{aligned}$$

Pero $d \mid |a|$ y $d \mid |b|$, así $d \mid |a| - |b|$.
$\therefore$ Esto cumple la condición. ■

Teorema 1.2. *Sean a y b números enteros, existe solo un número $d \in \mathbb{Z}$ tal que*

1) $d \geqslant 0$.

2) $d \mid a$ *y* $d \mid b$.

3) *Si $e \mid a$ y $e \mid b$, entonces $e \mid d$ para cualquier $e \in \mathbb{Z}$.*

Prueba: Por la definición 1.2 y por el teorema 1.1, existe un d con las siguientes propiedades:

$$d \mid a \qquad\qquad d \mid b \qquad\qquad d = ax + by$$

Es claro que $-d$ también cumple esto. Elegimos $|d| = ax' + by'$ que cumpla 1) y 2).

Si $e \mid a$ y $e \mid b$, entonces de la propiedad 3) $e \mid ax' + by' = |d|$.
Así, $e \mid |d|$, en consecuencia $e \mid d$ y $|d|$ satisface 3).
Si existiese un d' que cumpla 1), 2) y 3), entonces de la afirmación 3):

$$d \mid a \text{ y } d \mid b \implies d \mid d'.$$

De forma similar:

$$d' \mid a \text{ y } d' \mid b \implies d' \mid d.$$

Pero de la propiedad 10) ■