

Apuntes de Teoría de números^{*}

Estudiante Oromion^{**}

Actualizado a la fecha 13 de enero del 2018

^{*}Gracias al Grupo Estudiantil de Matemática y al Instituto de Matemática y Ciencias Afines.

^{**}E-mail: caznaranl@uni.pe.

Capítulo 1

Introducción

I. Principio de inducción matemática

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

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

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

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

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

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

como $a \mid n$.

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

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 $|d| \leq |n|$.
- 10) Si $d \mid n$ y $n \mid d$, entonces $|d| = |n|$.
- 11) Si $d \mid n$ con $d \neq 0$, entonces $\left(\frac{n}{d}\right) \mid n$.

1.2. 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 $K = 0, 1, \dots, n - 1$. (Hipótesis de inducción matemática).

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

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

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

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

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

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

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) $d \geq 0$.
- 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:

$$d \mid a$$

$$d \mid b$$

$$d = ax + by$$

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):

$$d \mid a \text{ y } d \mid b \implies d \mid d'. \quad (1.1)$$

De forma similar:

$$d' \mid a \text{ y } d' \mid b \implies d' \mid d. \quad (1.2)$$

Pero de (1.1) y (1.2) junto con la propiedad 10) se obtiene que $d = d'$. ■

Definición 1.3. Este número d es llamado máximo común divisor de a y b y se denota como $\text{mcd}(a, b)$ o (a, b) .

Observación 1.1. Si $\text{mcd}(a, b) = 1$, entonces a y b son llamados co-primos, primos entre sí (PESI) o primos relativos.

Algunas propiedades del máximo común divisor

- 1) $(a, b) = (b, a)$.
- 2) $(a, (b, c)) = ((a, b), c)$.
- 3) $(ac, bc) = |c|(a, b)$.
- 4) $(a, 1) = (1, a) = 1$.
- 5) $(a, 0) = (0, a) = |a|$.

Teorema 1.3. Si $a \mid bc$ y si $(a, b) = 1$, entonces $a \mid c$.

Demostración. Como $(a, b) = 1$, entonces existen $\tilde{x}, \tilde{y} \in \mathbb{Z}$ de modo que

$$1 = a\tilde{x} + b\tilde{y} \quad (1.3)$$

Pero si multiplicamos (1.3) por c resulta

$$c = a(c\tilde{x}) + b(c\tilde{y}) \quad (1.4)$$

Así, $a \mid cx$ y $a \mid cy$ (explicar).

■

1.3. Números primos

Definición 1.4. El número $n \in \mathbb{N}$ es llamado *número primo* si sus divisores positivos son 1 y n . Cuando n no es primo, será llamado *número compuesto*.

Teorema 1.4. Cada natural $n > 1$ o es primo o producto de números primos.

Prueba: Por inducción sobre n .

Para $n = 2$ ✓

Supongamos que se cumple para $n = 2, 3, \dots, k - 1$.

Demostraremos para $n = k$.

- *) Si k es un número primo.
- *) Si k no es un número primo, entonces k tiene por lo menos un divisor $d > 1$, por lo que $k = d \cdot c$ con $1 < c < k$ y $1 < d < k$.

Se cumple la hipótesis para c y d , entonces c y d son primos o productos de primos.

$$c = p_1 p_2 \cdots p_k \quad (p_i : \text{primo}, k \geq 1).$$

$$d = q_1 q_2 \cdots q_m \quad (q_i : \text{primo}, m \geq 1).$$

Así, $n = c \cdot d = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_m$ (se cumple la inducción).

■

Teorema 1.5. *Existen infinitos números primos.*

Prueba: Supongamos que $\mathbb{P} = p_1 p_2 \cdots p_k$ es el conjunto de todos los números primos que existen. Definimos:

$$N = p_1 p_2 \cdots p_k + 1$$

¿Qué tipo de número es N , es un primo o uno compuesto?

Claro está que N es mayor que $p_i, \forall i = 1, \dots, k$.

$$N = p_1 p_2 \cdots p_k + 1 = q_1 q_2 \cdots q_t.$$

$$\begin{array}{r} q_i \mid p_1 p_2 \cdots p_k + 1 \\ q_i \mid p_1 p_2 \cdots p_k \\ \hline q_i \mid 1 \quad (\implies \Longleftarrow) \end{array} \quad (-)$$

\therefore Existen infinitos números primos. ■

Teorema 1.6. *Si p es un número primo y $p \nmid a$, entonces $(p, a) = 1$.*

Demostración. Sea d el máximo común divisor de p y a (ya que el teorema 1.1 nos asegura su existencia), $d = (p, a)$, entonces

$$d \mid p \quad \text{y} \quad d \mid a.$$

■

Teorema 1.7. *Sea p un número primo. Si $p \mid ab$, entonces $p \mid a$ o $p \mid b$.*

Demostración: Supongamos que $p \nmid a$ ($p \nmid a$ ✓), entonces $(p, a) = 1$, en consecuencia, $p \mid ab$.

$$a \mid bc \quad \text{y} \quad (a, b) = 1 \implies a \mid c.$$

$\therefore p \mid b$. ■

Teorema 1.8. *Cada entero $n > 1$ se representa de forma única como producto de primos no necesariamente distintos, sin importar el orden.*

Prueba: Por inducción en n . Cuando $n = 2$ (se cumple: $2, 3, \dots, n-1$.) $n = p_1 p_2 \cdots, p_s = q_1 q_2 \cdots q_t$ ($s = t$). ($s, t \geq 1$)

$$p_1 \mid q_1 q_2 \cdots q_t \implies p_1 \mid q_1 \implies p_1 = q_1. \quad \blacksquare$$

Observación 1.2. Si se desea representar a n como producto de primos distintos (donde cabe la posibilidad en que se repitan algún número primo), podemos escribir:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = \prod_{i=1}^k p_i^{a_i}$$

Teorema 1.9. Si $n = \prod_{i=1}^r p_i^{a_i}$, entonces un divisor de n tiene la forma

$$\prod_{i=1}^r p_i^{c_i}, \quad 0 \leq c_i \leq a_i.$$

Observación 1.3. Sea la sucesión de números primos

$$p_1 = 2, p_2 = 3, p_3 = 5, \dots,$$

$$\text{entonces } n = \prod_{i=1}^{\infty} p_i^{a_i}, \quad a_i \geq 0.$$

Teorema 1.10. Sean $a = \prod_{i=1}^{\infty} p_i^{a_i}$ y $b = \prod_{i=1}^{\infty} p_i^{b_i}$, entonces el máximo común divisor de a y b es

$$(a, b) = \prod_{i=1}^{\infty} p_i^{c_i} \geq 0, \text{ donde } c_i = \min\{a_i, b_i\} \leq a_i, b_i.$$

$$\text{Demostración:} \quad *) \quad \prod_{i=1}^{\infty} p_i^{c_i} \mid a \quad \wedge \quad \prod_{i=1}^{\infty} p_i^{c_i} \mid b.$$

$$*) \quad e \mid a \quad \wedge \quad e \mid b, e = \prod_{i=1}^{\infty} p_i^{e_i}.$$

Pero, $e_i \leq a_i$ y $e_i \leq b_i$,

$$\implies e_i \leq \min\{a_i, b_i\} = c_i.$$

