Aritmética de los Enteros

Ronald Mas,
Angel Ramirez

12 de agosto de 2020

Contenido

Introducción

El conjunto de los números enteros $\mathbb{Z}$ posee una estructura que nos permite hablar de factorización única, divisibilidad, múltiplos (ideales). Es más de acuerdo al número de sus divisores se puede definir los números primos. El siguiente cuadro muestra las bondades que posee $\mathbb{Z}$:

	Suma	Producto
Clausura	✓	✓
Neutro	✓	✓
Inverso	✓	X
Asociatividad	✓	✓

Los únicos elementos que poseen inverso multiplicativo son el -1 y 1. Es más, se cumple la propiedad distributiva y que carece de elementos divisores de 0. Existen otros conjunto con las mismas características de $\mathbb{Z}$, estos reciben el nombre de **dominio de factorización única**.

Teorema (Teorema de Representación Base)

Sea $b > 1$ un número entero. Entonces para cada $n \in \mathbb{N}$ existe una sucesión de números enteros no negativos $\{a_i\}_{i=0}^{m}$ tal que:

$$n = \sum_{i=0}^{m} a_i b^i$$

con $0 \leq a_i < b$, $\forall j \in \{0, 1, \cdots, m\}$ y $a_m \neq 0$.
Es más esta representación es única y es llamada **la representación de** n **en base** b.

Prueba:

Procedamos por inducción fuerte sobre n:

1) Para $n = 1$ se tiene que $a_0 = 1$, luego $n = a_0$.

Continuación de la prueba

2) Supongamos que todo número entero menor que n se puede representar en base b, luego por el algoritmo de Euclides existen únicos q, r enteros tal que

$$n = qb + r, \text{ con } 0 \leq r < b.$$

Por hipotesis de inducción sobre $q < n$ se tiene que:

$$q = \sum_{i=0}^{m} a'_i b^i$$

para alguna sucesión $\{a'_i\}_{i=0}^{m}$ con $0 \leq a'_i < b$. Luego

$$n = (\sum_{i=0}^{m} a'_i b^i)b + r = \sum_{i=0}^{m} a'_i b^{i+1} + r$$

Por tanto, al considerar $a_0 = r$ y $a_{i+1} = a'_i$ se tiene el resultado deseado.

Máximo común divisor y mínimo común múltiplo

Definición

Dados $a, b \in \mathbb{Z}$ con $a \neq 0$, decimos que a divide a b si existe $c \in \mathbb{Z}$ tal que $b = ac$. En adelante a divide a b se denota como $a \mid b$.

Definición

Dados $a, b \in \mathbb{Z}$ no nulos, decimos que $d \in \mathbb{Z}^+$ es el máximo común divisor de a y b:

1) $d \mid a$ y $d \mid b$.
2) Si existe $d' \in \mathbb{Z}$ tal que $d' \mid a$ y $d' \mid b$ entonces $d' \mid d$.

En adelante denotamos $d = MCD(A, B)$.

Observación:

- Si existe el MCD de a y b este es único.

Teorema (Existencia del MCD)

Si $a, b \in \mathbb{Z}$ no nulos entonces existe $MCD(a, b)$ y $MCD(a, b) = m_0 a + n_0 b$ para algunos $m_0, n_0 \in \mathbb{Z}$.

Prueba:

Sea

$$I = \{ma + nb : \ m, n \in \mathbb{Z}\}$$

- **Afirmación 1**: $I \neq \emptyset$.
  En efecto, $a = 1.a + 0.b$ y $b = 0.a + 1.b$ de aquí se tiene que $a, b \in I$ entonces $-x = ((-m)a + (-n)b) \in \mathbb{Z}$, por tanto $I \cap \mathbb{Z}^+ \neq \emptyset$.
  Luego por el principio de buen orden existe $d \in I \cap \mathbb{Z}^+$ tal que $d \leq x$, $\forall x \in I \cap \mathbb{Z}^+$ entonces existen $m_0, n_0 \in \mathbb{Z}$ tal que $d = (m_0 a + n_0 b)$ con $0 < d \leq x$, $\forall x \in I \cap \mathbb{Z}^+$.

Continua la prueba

- **Afirmación 2**: $d = MCD(a, b)$.

  1) Si $x = (ma + nb) \in I$, por el algoritmo de la división existen únicos $q, r \in \mathbb{Z}$ tales que $x = dq + r$ con $0 \leq r < d$ entonces $ma + nb = (m_0 a + n_0 b)q + r$ de donde se concluye que $r = ((m - m_0 q)a) + ((n - n_0 q)b) \in I$.
  Como $r \in I$ con $r \geq 0$ entonces $r = 0$ (caso contrario se contradice la minimalidad de d). Por lo tanto $x = dq$, así $d \mid x$, $\forall x \in I$. Luego en particular $d \mid a$ y $d \mid b$.
  2) Si $d' \mid a$ y $d' \mid b$ entonces $d' \mid (m_0 a + n_0 b)$, es decir $d' \mid d$.

Definición

Sean $a, b \in \mathbb{Z}$ no nulos, decimos que a y b son primos relativos si $MCD(a, b) = 1$.

Definición

Sea $p \in \mathbb{Z}$, decimos que p es un número primo si posee exactamente 4 divisores enteros que son: ± 1 y $\pm p$.

Observaciones:

1) La cantidad de números primos en $\mathbb{Z}$ es infinito.
Prueba:
Es suficiente probar que la cantidad de números primos en $\mathbb{N}$ es infinita. Procedamos por contradicción, supongamos que la cantidad sea finita y este dada por el conjunto:

$$P = \{p_1, p_2, \cdots, p_k \ ; \text{tal que } p_1 \leq p_2 \leq \cdots p_k\}$$

Luego el elemento p_k es el máximo elemento que pertenece a P.
Por otro lado, $m = p_1.p_2 \cdots .p_k + 1 \in P$ ya que no es divisible por ningún elemento de P, pero $p_k < m$. Ello contradice la maximalidad de p_k.

Continua las observaciones

2) Sea $p \in \mathbb{Z}^+$ un número primo, se cumple:
   1. Si $p = 4k + 1$ con $k \in \mathbb{N}$ entonces p se puede expresar como suma de dos cuadrados.
   2. Si $p = 4k + 3$ con $k \in \mathbb{N}$ entonces p no se puede expresar como suma de dos cuadrados.

Prueba:
2. Todo número cuadrado perfecto al dividirlo entre 4 deja residuo 0 o 1, luego la suma de dos cuadrados perfectos dejan como residuo de dividir entre 4 a $0, 1$ o 2. Por ello ningún primo de la forma $4k + 3$ con $k \in \mathbb{N}$ se puede expresar como suma de dos cuadrados.

A pesar de no ser objeto de estudio en el curso, la última observación juega un papel importante en el estudio de los números primos en los enteros gaussianos $\mathbb{Z}(i) = \{a + bi : a, b \in \mathbb{Z}\}$ ya que permite establecer que números primos en $\mathbb{Z}$ dejan de serlo en $\mathbb{Z}(i)$. Por ejemplo 5 es un número primo en $\mathbb{Z}$ pero no lo es $\mathbb{Z}(i)$ ya que $5 = (1 - 2i)(1 + 2i)$.

Lema (1)

Sean $a, b, c \in \mathbb{Z}$ no nulos. Si $a \mid bc$ y $MCD(a, b) = 1$ entonces $a \mid c$.

Prueba:

Como $MCD(a, b) = 1$ entonces existen $r, s \in \mathbb{Z}$ tal que $ra + sb = 1$ entonces $rac + sbc = c$ y como $a \mid bc$ se tiene que $a \mid c$.

Lema (2)

Si $a \in \mathbb{Z}$ y $p \in \mathbb{Z}$ es un número primo entonces $p \mid a$ o $MCD(a, p) = 1$.

Prueba:

Si $p \mid a$ no hay nada que probar. Supongamos que $p \nmid a$ y sea $d = MCD(a, p)$ entonces $d \mid p$ y $d \mid a$. Luego $d = 1$ (termina la prueba) o $d = p$, si $d = p$ entonces $p \mid a$, ello es un contradicción.

Lema (3)

Sean $a, b \in \mathbb{Z}$ no nulos y $p \in \mathbb{Z}$ primo. Si $p \mid ab$ entonces $p \mid a$ o $p \mid b$.

Prueba:

Si $p \mid a$, termina la prueba. Supongamos que $p \nmid a$ entonces por el lema anterior $MCD(a, p) = 1$ y como $p \mid ab$, se tiene por el lema (1) que $p \mid b$.

Teorema (Teorema Fundamental de la Aritmética)

Todo número $n \in \mathbb{Z}$ no nulo puede ser escrito de forma única como:

$$n = \mu p_1 p_2 \cdots p_k$$

donde $\mu \in \{-1, 1\}$ y $p_1 \leq p_2 \cdots \leq p_k$ son números primos enteros positivos (no necesariamente distintos).

1) **Existencia**:
Es suficiente probar para $n \in \mathbb{N}$ $(\mu = 1)$, procedamos por inducción.
   - Si $n = 1$ se tiene que $n = \mu p_1 p_2 \cdots p_k$ con $\mu = 1$ y $k = 0$.
   - Supongamos que todo entero m con $1 \leq m < n$ puede ser escrito coo producto de primos. Si n es primo la prueba termina, caso contrario existen $d, d' \in \mathbb{Z}$ tal que $n = dd'$ con $1 < d, d' < n$. Luego por hipotesis inductiva se tiene:

$$\begin{array}{lll} d = q_1 q_2 \cdots q_r & \text{con} & q_1 \leq q_2 \leq \cdots \leq q_r \text{ primos positivos y} \\ d' = q_1' q_2' \cdots q_s' & \text{con} & q_1' \leq q_2' \leq \cdots \leq q_s' \text{ primos positivos.} \end{array}$$

   Al reemplazar y ordenar si fuese necesario los primos $q_1, q_2, \cdots, q_r, q_1', q_2', \cdots q_s'$ se tiene el resultado deseado con $k = r + s$.

2) **Unicidad:**

Supongamos que

$$n = \mu p_1 p_2 \cdots p_k = \mu' p_1' p_2' \cdots p_s' \text{ con}$$

$p_1 \leq p_2 \leq \cdots \leq p_k$ y $p_1' \leq p_2' \leq \cdots \leq p_s'$ primos positivos entonces $\mu = \mu'$ y $p_1 p_2 \cdots p_k = p_1' p_2' \cdots p_s'$, faltaría probar que $k = s$ y que $p_i = p_i'$, $\forall i \in \{1, 2, \cdots, k\}$. Procedamos por inducción sobre k.

- Si $k = 1$ entonces $p_1 = p_1' p_2' \cdots p_s'$, luego $p_s' \mid p_1$, por tanto $p_s' = p_1$ (s=1 y $p_1' = p_1$).
- Supongamos que para r factores primos positivos con $1 \leq r < k$ se cumple la unicidad. Luego como:

$$\begin{array}{lll} p_1 \mid p_j' & \text{para algún } j \text{ tal que} 1 \leq j \leq s & \text{entonces } p_1 = p_j' \\ p_1' \mid p_i & \text{para algún } i \text{ tal que} 1 \leq i \leq k & \text{entonces } p_1' = p_i \end{array}$$

y $p_1 \leq p_2 \leq \cdots \leq p_k$ y $p_1' \leq p_2' \leq \cdots \leq p_s'$ se tiene que $p_1 = p_1'$. Entonces $p_2 p_3 \cdots p_k = p_2' p_3' \cdots p_s'$ y hipotesis inductiva aplicada a $r = k - 1$ se tiene que $k - 1 = s - 1$ y $p_2 = p_2', p_3 = p_3', \cdots, p_k = p_k'$. Por tanto $k = s$ y $p_i = p_i'$, $\forall i \in \{1, 2, \cdots, k\}$.