Aritmética Modular

Ronald Mas,
Angel Ramirez

14 de agosto de 2020

Contenido

Teorema (Teorema chino del resto)

Sean $n_1, n_2, \cdots, n_k \in \mathbb{N}$, k *números naturales con* $k > 1$ *tal que:*

$$MCD(n_i, n_j) = 1, \ \forall i \neq j$$

y $r_i \in \mathbb{Z}$, *donde* $i \leq k$ *son arbitrarios. Entonces existen enteros* x_i, *donde* $1 \leq i \leq k$ *tal que:*

$$n_1x_1 + r_1 = n_2x_2 + r_2 = \cdots = n_kx_k + r_k. \tag{1}$$

Prueba:

Procedamos por inducción sobre k. Si $k = 2$, se tiene $MCD(n_1, n_2) = 1$ entonces existen $z_1, z_2 \in \mathbb{Z}$ tal que $n_1z_1 + n_2z_2 = 1$. Luego la ecuación $n_1x - n_2y = r_2 - r_1$ tiene solución, la cuál es $(x_1, x_2) = (z_1(r_2 - r_1), z_2(r_1 - r_2))$. Supongamos que el resultado es cierto para $k \geq 2$, veamos para $k + 1$.

Sean $n_1, n_2, \cdots, n_{k+1} \in \mathbb{N}$ números primos relativos dos a dos y $r_1, r_2, \cdots, r_{k+1} \in \mathbb{Z}$ elegidos arbitrariamente.

Continua la prueba

Por hipotesis de inducción, existen enteros $x_1, x_2, \cdots, x_k \in \mathbb{Z}$ que satisfacen la ecuación (1). Como los n_i con $1 \leq i \leq k$ son primos relativos dos a dos entonces $n_1 n_2 \cdots n_k$ y n_{k+1} son primos relativos también, es decir $MCD(n_1 n_2 \cdots n_k, n_{k+1}) = 1$, luego existen $X, Y \in \mathbb{Z}$ tal que $n_1 n_2 \cdots n_k X - n_{k+1} Y = r_{k+1} - n_1 x_1 - r_1$.
Al considerar

$$X_j = \frac{n_1 n_2 \cdots n_k X}{n_j} + x_j \in \mathbb{Z} \; \forall 1 \leq j \leq k \text{ y } X_{k+1} = Y,$$

se tiene $n_1 X_1 + r_1 = n_2 X_2 + r_2 = \cdots = n_{k+1} X_{k+1} + r_{k+1}$.

Los Enteros Módulo n

Sea $n \in \mathbb{Z}^+$, $n \geq 2$ se define la relación $\equiv_n$ sobre $\mathbb{Z}$ como:

$$a \equiv_n b \text{ si y sólo si } n \mid (a - b).$$

Es bien sabido que dicha relación es de equivalencia. Por tanto, la clase de a y el conjunto cociente son respectivamente:

$$\overline{a} = \{a + kn : \ k \in \mathbb{Z}\} \text{ y}$$

$$\mathbb{Z}_n := \frac{\mathbb{Z}}{\equiv_n} = \{\overline{a} : \ a \in \mathbb{Z}\}$$

Proposición

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\} \text{ y } \mid \mathbb{Z}_n \mid = n.$$

Prueba: Si $x \in \mathbb{Z}_n$ entonces $x = \overline{a}$ con $a \in \mathbb{Z}$, luego por el algoritmo de la división existen $q, r \in \mathbb{Z}$ tal que $a = qn + r$, $0 \leq r < n$, es decir existe $r \in \mathbb{Z}$, $0 \leq r < n$ tal que $a \equiv_n r$ entonces $x = \overline{a} = \overline{r}$. Luego $x \in \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$, es decir:

$$\mathbb{Z}_n \subseteq \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}.$$

Por tanto

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}.$$

Por otro lado veamos que $\mid \mathbb{Z}_n \mid = n$, supongamos que existen $i, j \in \mathbb{Z}$ tal que $0 \leq i < j < n$ y $\overline{i} = \overline{j}$ entonces $j - i = n\alpha$, $\alpha \in \mathbb{Z}$ y como $0 < j$ y $i < n$ se tiene que $0 < n\alpha < n$ entonces $0 < \alpha < 1$ con $\alpha \in \mathbb{Z}$, lo cuál es una contradicción.

Proposición

Sean $\overline{a}, \overline{a'}, \overline{b}, \overline{b'} \in \mathbb{Z}_n$. *Si* $\overline{a} = \overline{a'}$ *y* $\overline{b} = \overline{b'}$ *entonces*

$$\overline{a+b} = \overline{a'+b'} \text{ y } \overline{ab} = \overline{a'b'}.$$

Prueba:

Como $\overline{a} = \overline{a'}$ y $\overline{b} = \overline{b'}$ entonces $n \mid (a-a')$ y $n \mid (b-b')$. Luego, como $(a+b)-(a'+b') = (a-a')+(b-b')$ se tiene que $n \mid [(a+b)-(a'+b')]$, así $\overline{a+b} = \overline{a'+b'}$. Por otro lado, como $ab - a'b' = (a-a')b + a'(b-b')$ se tiene que $n \mid (ab-a'b')$, así $\overline{ab} = \overline{a'b'}$.

Definición

En $\mathbb{Z}_n$ definamos las operaciones:

$$\overline{a} \oplus \overline{b} = \overline{a+b} \text{ y } \overline{a} \odot \overline{b} = \overline{ab}$$

La proposición anterior nos garantiza la buena definición de estas operaciones. Por abuso de notación $\oplus$ y $\odot$las denotamos por $+$ y .

Teorema

Las operaciones en $\mathbb{Z}_n$ satisfacen las siguientes propiedades:

1) $\overline{x} + (\overline{y} + \overline{z}) = (\overline{x} + \overline{y}) + \overline{z},\ \forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_n.$
2) $\exists \overline{0} \in \mathbb{Z}_n :\ \overline{x} + \overline{0} = \overline{0} + \overline{x} = \overline{x},\ \forall \overline{x} \in \mathbb{Z}_n.$
3) $\forall \overline{x} \in \mathbb{Z}_n,\ \exists (-\overline{x}) \in \mathbb{Z}_n :\ \overline{x} + (-\overline{x}) = (-\overline{x}) + \overline{x} = \overline{0}.$
4) $\overline{x} + \overline{y} = \overline{y} + \overline{x},\ \forall \overline{x}, \overline{y} \in \mathbb{Z}_n.$
5) $(\overline{x}\,\overline{y})\overline{z} = \overline{x}(\overline{y}\,\overline{z}),\ \forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_n.$
6) $\exists \overline{1} \in \mathbb{Z}_n$: $\overline{x}\overline{1} = \overline{1}\overline{x} = \overline{x},\ \forall \overline{x} \in \mathbb{Z}_n.$
7) $\overline{x}\,\overline{y} = \overline{y}\,\overline{x},\ \forall \overline{x}, \overline{y} \in \mathbb{Z}_n.$
8) $\overline{x}(\overline{y} + \overline{z}) = \overline{x}\,\overline{y} + \overline{x}\,\overline{z},\ \forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_n.$

Prueba:

2) $\overline{0} = \{0 + kn : \ k \in \mathbb{Z}\} = \{kn : \ k \in \mathbb{Z}\} = \{0, \pm n, \pm 2n, \cdots\}$ y es claro que:

$$\overline{x} + \overline{0} = \overline{x + 0} = \overline{x}, \ \overline{0} + \overline{x} = \overline{0 + x} = \overline{x}, \ \forall \overline{x} \in \mathbb{Z}_n.$$

3) $\overline{x} + (-\overline{x}) = \overline{x + (-x)} = \overline{0}$ y $\overline{(-x)} + \overline{x} = \overline{(-x) + x} = \overline{0}, \ \forall \overline{x} \in \mathbb{Z}_n.$

8) $\overline{x}(\overline{y} + \overline{z}) = \overline{x}\overline{(y + z)} = \overline{x(y + z)} = \overline{xy} + \overline{xz} = \overline{x}\,\overline{y} + \overline{x}\,\overline{z}, \ \forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_n.$

Proposición

En $\mathbb{Z}_n$ se cumple que:

1) *Si $\overline{x} \neq \overline{0}$ y $\overline{y} \neq \overline{0}$ entonces $\overline{x}\,\overline{y} \neq \overline{0}$ si y sólo si n es primo.*
2) *Si n es un número primo, para cada $\overline{x} \in \mathbb{Z}_n - \{0\}$, existe $\overline{y} \in \mathbb{Z}_n$ tal que $\overline{x}\,\overline{y} = \overline{y}\,\overline{x} = \overline{1}$.*

Prueba:

2) Sea $\overline{x} \in \mathbb{Z}_n$ con $\overline{x} \neq \overline{0}$ entonces $MCD(p, x) = 1$, por tanto existen $r, s \in \mathbb{Z}$ tal que $pr + xs = 1$, luego $\overline{x}\,\overline{s} = \overline{1}$. Por lo tanto $\exists \overline{y} = \overline{s} \in \mathbb{Z}_n$ tal que $\overline{x}\,\overline{y} = \overline{1}$.

Continua prueba

1) $\Rightarrow$) Si $d \mid n$ entonces $n = db$ con $b \in \mathbb{Z}$, así $\overline{db} = \overline{0}$ entonces $\overline{d} = \overline{0}$ o $\overline{b} = \overline{0}$, analicemos ambos casos:
   - Si $\overline{d} = \overline{0}$ entonces $n \mid d$, y como $d \mid n$ se tiene que $d = \pm n$.
   - Si $\overline{b} = \overline{0}$ entonces $n \mid b$, es decir $b = n\beta$ con $\beta \in \mathbb{Z}$, luego como $n = db$ entonces $n = dn\beta$, así $1 = d\beta$, por ello $d = \pm 1$. Por tanto n es primo.

   $\Leftarrow$) Si n es primo y $\overline{a}\,\overline{b} = \overline{0}$ en $\mathbb{Z}_n$ entonces $n \mid ab$, luego $n \mid a$ o $n \mid b$, así se tiene que $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$.

Observaciones:

- Por la parte 2) de la proposición anterior, se tiene que todo elemento dinstinto de $\overline{0}$ en $\mathbb{Z}_p$ con p primo posee inverso multiplicativo, en particular decimos que $\mathbb{Z}_p$ es un **cuerpo**.

Ejemplo 1:

Para $n = 12$, se tiene que en $\mathbb{Z}_{12}$ la siguiente tabla:

	Inverso aditivo	Inverso multiplicativo
$\bar{0}$	$\bar{0}$	No tiene
$\bar{1}$	$\bar{11}$	$\bar{1}$
$\bar{2}$	$\bar{10}$	No tiene
$\bar{3}$	$\bar{9}$	No tiene
$\bar{4}$	$\bar{8}$	No tiene
$\bar{5}$	$\bar{7}$	$\bar{5}$
$\bar{6}$	$\bar{6}$	No tiene
$\bar{7}$	$\bar{5}$	$\bar{7}$
$\bar{8}$	$\bar{4}$	No tiene
$\bar{9}$	$\bar{3}$	No tiene
$\bar{10}$	$\bar{2}$	No tiene
$\bar{11}$	$\bar{1}$	$\bar{11}$

Ejemplo 2:

Para $n = 13$, se tiene que en $\mathbb{Z}_{13}$ la siguiente tabla:

	Inverso aditivo	Inverso multiplicativo
$\bar{0}$	$\bar{0}$	No tiene
$\bar{1}$	$\bar{12}$	$\bar{1}$
$\bar{2}$	$\bar{11}$	$\bar{7}$
$\bar{3}$	$\bar{10}$	$\bar{9}$
$\bar{4}$	$\bar{9}$	$\bar{10}$
$\bar{5}$	$\bar{8}$	$\bar{8}$
$\bar{6}$	$\bar{7}$	$\bar{11}$
$\bar{7}$	$\bar{6}$	$\bar{2}$
$\bar{8}$	$\bar{5}$	$\bar{5}$
$\bar{9}$	$\bar{4}$	$\bar{3}$
$\bar{10}$	$\bar{3}$	$\bar{4}$
$\bar{11}$	$\bar{2}$	$\bar{6}$
$\bar{12}$	$\bar{1}$	$\bar{12}$