Los enteros módulo n

Recordemos que para $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^*$ decimos que a es congruente con b módulo n y lo denotamos

$$a \equiv b \pmod{n} \quad \text{o} \quad a \equiv b \ (n)$$

si la diferencia $a-b$ es divisible por n, o lo que es lo mismo, si existe $k \in \mathbb{Z}$ tal que

$$a - b = k \cdot n$$

$$a = b + k \cdot n$$

La congruencia módulo n es una relación de equivalencia en $\mathbb{Z}$, es decir

- Reflexiva: $a \equiv a \ (n) \quad \forall a \in \mathbb{Z}$
- Simétrica: si $a \equiv b \ (n)$ entonces $b \equiv a \ (n) \quad \forall a,b \in \mathbb{Z}$
- Transitiva: si $a \equiv b \ (n)$ y $b \equiv c \ (n)$ entonces $a \equiv c \ (n) \quad \forall a,b,c \in \mathbb{Z}$.

Ejercicio: Probar que $\ldots \equiv \ldots \ (n)$ es una relación de equivalencia.

Al ser una relación de equivalencia en $\mathbb{Z}$, particiona a todo el conjunto en clases disjuntas, n clases

$$[a] = \{b \in \mathbb{Z} : a \equiv b \ (n)\} \leftarrow \text{clase de } a$$

$a \in \mathbb{Z}$

$b-0$ es divisible por n, $n \mid b-0 = b$

$$[0] = \{ b \in \mathbb{Z} : \overbrace{b \equiv 0 \ (n)} \} =$$

$$= \{ b \in \mathbb{Z} : b = k.n \quad k \in \mathbb{Z} \}$$

$$= \{ \ldots -2n, -n, 0, n, 2n, 3n, 4n, \ldots \}$$

$$[1] = \{ b \in \mathbb{Z} : b \equiv 1 \ (n) \}$$

$$= \{ b \in \mathbb{Z} : b = k.n+1, \text{ para } k \in \mathbb{Z} \}$$

$$= \{ \ldots -2n+1, -n+1, 1, n+1, 2n+1, 3n+1, \ldots \}$$

$$[2] = \ldots$$

$$\vdots$$

$$[n-1] = \{ b \in \mathbb{Z} : b \equiv n-1 \ (n) \}$$

$$= \{ b \in \mathbb{Z} : b = k.n + (n-1) \}$$

$$= \{ \ldots, -n-1, -1, n-1, 2n-1, \ldots \}$$

Por ejemplo si pensamos en $n=6$

$$[0] = \{\dots, -12, -6, 0, 6, 12, \dots\} = [24]$$

$$(-5) = [1] = \{\dots, -11, -5, 1, 7, 13, \dots\} \qquad -11 = (-2)\cdot 6 + 1$$

$$[8] = [2] = \{\dots, -10, -4, 2, 8, 14, \dots\}$$

$$[3] = \{\dots, -9, -3, 3, 9, 15, \dots\}$$

$$[4] = \{\dots, -8, -2, 4, 10, 16, \dots\}$$

$$[5] = \{\dots, -7, -1, 5, 11, 17, \dots\}$$

$$[5] = \bar{5} = 5$$

Consideremos el conjunto $\{[0], [1], \dots, [n-1]\}$ y definamos la suma de dos clases como

$$[a] + [b] = [a+b]$$

Por ejemplo $[2] + [4] = [2+4] = [6] = [0]$.

Veamos que esta suma está bien definida, es decir que no depende del representante elegido.

Tenemos que mostrar que $[a] = [a']$ y $[b] = [b']$

$$[a] + [b] = [a'] + [b'].$$

Si $[a]=[a']$ entonces $a-a' = k_1 \cdot n$ para algún $k_1 \in \mathbb{Z}$

$a = k_1 \cdot n + a'$

Si $[b]=[b']$ entonces existe $k_2 \in \mathbb{Z}$ tal que $b = k_2 \cdot n + b'$

$$[a]+[b] = [a+b] = [(k_1 n + a') + (k_2 n + b')] =$$

$$= [(k_1+k_2)n + (a'+b')] = [a'+b'] = [a']+[b'].$$

Por ejemplo continuando con el caso $n=6$

$$[2]+[4] = [6] = [0]$$

$$[8]+[4] = [8+4] = [12] = [0].$$

Ejercicio.

$\left(\{[0], [1], \ldots, [n-1]\}, +\right)$ es un grupo abeliano.

El grupo anterior se llama el grupo de los enteros módulo n y lo denotamos $\mathbb{Z}_n$.

De manera similar podemos definir el producto de clases

$$[a].[b] = [a.b]$$

$[0] = [a] + [b] = [a+b]$ $\qquad [-a] =$

$[2] + [-2] =$

$a+b = k.n$

$[a] + [0] = [a+0] = [a]$

Ejercicio: Probar que está bien definido.

Ejercicio:

$(\mathbb{Z}_n, +, \cdot)$ es un anillo conmutativo con unidad.

En general, $(\mathbb{Z}_n, +, \cdot)$ no es un dominio integral.

Ejemplo: $(\mathbb{Z}_6, +, \cdot)$

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]						
[4]						
[5]						

·	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]		
[3]						
[4]						
[5]						

divisores (propios) de cero.

Por ejemplo $[2] \neq [0]$, $[3] \neq [0]$ pero $[2].[3] = [0]$.

Observar que si recordamos la definición de cuerpo, tenemos que todo cuerpo es un dominio integral.

Supongamos que un cuerpo $(F, +, \cdot)$ tengo dos elementos $a, b \in F$ tales que $a \cdot b = 0$. Supongamos que $a \neq 0$.

Como F es un cuerpo y $a \neq 0$ existe a^{-1} inverso multiplicativo de a

$$a^{-1}(a \cdot b) = a^{-1} \cdot 0$$

$$(a^{-1} \cdot a) \cdot b = 0$$

$$b = 0.$$

Entonces todo cuerpo es un D.I.

La recíproca no es cierta porque por ejemplo $(\mathbb{Z}, +, \cdot)$ es un D.I. pero no es un cuerpo.

Pero, si se pide además que el anillo sea finito, entonces sí se cumple.

Teorema: Todo dominio integral finito es un cuerpo.

Dem.

Sea R un D.I. finito. Para que sea cuerpo debemos mostrar que si $a \in R$ y $a \neq 0$ entonces existe un $a^{-1} \in R$ tal que $a^{-1} \cdot a = 1$.

Como R es finito podemos escribir

$$R = \{a_1, a_2, \ldots, a_s\} \quad \text{con todos distintos.}$$

Consideremos ahora los productos

$$a_1 \cdot a, \; a_2 \cdot a, \; \ldots, \; a_s \cdot a$$

y como $a \neq 0$ entonces estos elementos son todos distintos. (si esto no fuera así tendríamos $a_i \cdot a = a_j \cdot a \Rightarrow (a_i - a_j) \cdot a = 0 \Rightarrow a_i = a_j$ ※)

Entonces, en particular, $1 = a_i \cdot a \Rightarrow a_i = a^{-1}$.

y por lo tanto, $(R, +, \cdot)$ es un cuerpo. ∎

Teorema: Para cualquier primo p, $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo.

Demostración.

Ya sabemos que $(\mathbb{Z}_n, +, \cdot)$ es un anillo conmutativo con unidad y finito. Vamos a probar que si $n = p$ primo entonces es un D.I.

Supongamos $[a], [b] \in \mathbb{Z}_p$ tales que

$$[a] \cdot [b] = [0]$$
$$\| $$
$$[a \cdot b]$$

Esto significa que p divide a $a \cdot b$.

$$p \mid a \cdot b \qquad a \cdot b = k \cdot p.$$

Como p es primo entonces $p \mid a$ o $p \mid b$.

entonces $[a] = [0]$ o $[b] = [0]$.

$\therefore$ $(\mathbb{Z}_p, +, \cdot)$ es un D.I. finito y por el teorema anterior es un cuerpo. ∎

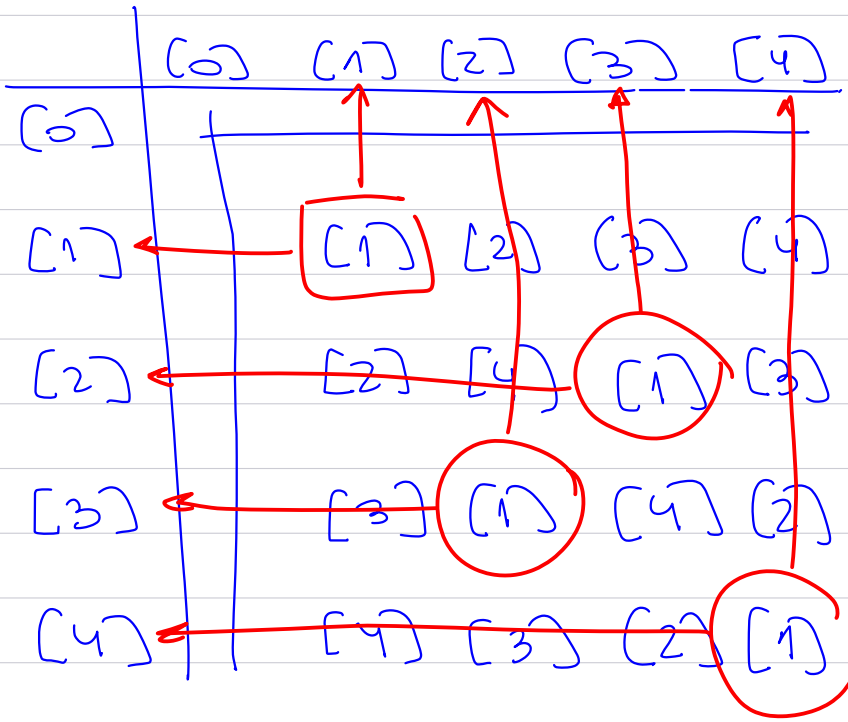
Ejemplo: $(\mathbb{Z}_5, +, \cdot)$

$[1]^{-1} = [1]$

$[2]^{-1} = [3]$

$[3]^{-1} = [2]$

$[4]^{-1} = [4]$.



Los enteros módulo un primo con la suma de clases y el producto de clases son ejemplos de cuerpos finitos.

Los cuerpos $\mathbb{F}_p$, p primo

Recordemos que una aplicación (o mapeo) $f: G \to H$ entre dos grupos $(G, *)$ y $(H, \cdot)$ se llama un homomorfismo de G en H si f preserva la operación en G, es decir si $\forall\, a, b \in G$

$$f(a * b) = f(a) \cdot f(b)$$

($*$: operación en G; $\cdot$: operación en H.)

Si además si f es sobreyectiva se llama epimorfismo

Si f es biyectiva (1a1 y sobre) entonces se llama isomorfismo.

Esta definición se extiende fácilmente al caso de anillos.

Def: Un mapeo $f: R \to S$ entre dos anillos $(R, +, \cdot)$ y $(S, +', \cdot')$ es un homomorfismo de anillos

$$f(a+b) = f(a) +' f(b) \quad \text{y} \quad f(a \cdot b) = f(a) \cdot' f(b)$$

Estos mapas pueden usarse para transferir estructuras desde un anillo a un conjunto sin estructura. Por ejemplo si $(R,+,\cdot)$ es un anillo y S es un conjunto de manera que hay un $f: R \to S$ que sea 1 a 1 y sobre, podemos transferir la estructura de R a S convirtiendo a f en un isomorfismo.

Para $s_1, s_2 \in S$ definimos $\left(\exists\, r_1, r_2 \in R \,/\, \begin{matrix} f(r_1)=s_1 \\ f(r_2)=s_2 \end{matrix}\right)$

$$s_1 \oplus s_2 = f(r_1) + f(r_2)$$

$$s_1 \odot s_2 = f(s_1) \cdot f(s_2)$$

En este caso decimos que S tiene una estructura de anillo inducida por f (o por R).

Def: Para un primo p, sea $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ y consideremos la aplicación $f: \mathbb{Z}_p \to \mathbb{F}_p$

$$f([a]) = a \bmod p = \tilde{a} \quad \text{con} \quad 0 \le \tilde{a} \le p-1.$$

$\mathbb{F}_p$ posee la estructura de cuerpo inducida por f.

$(\mathbb{F}_p, +, \cdot)$ es un cuerpo finito de órden p.