Vídeo : `https://youtu.be/PFXWULTmk44`

1. Resumen

Empezaremos viendo cómo calcular las tablas de sumar y multiplicar en $\mathbb{Z}_5$ que vimos anteriormente.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Dados dos números a y b, para calcular su suma, resta o su producto en $\mathbb{Z}_5$ se realiza dicha operación como números enteros ordinarios y luego se suman o se restan múltiplos de 5 hasta dejar el resultado en $\{0, 1, 2, 3, 4\}$.
Esta regla nos lleva a la definición general:

Definición 1. *Sea n entero positivo y sean $a, b \in \mathbb{Z}$. Diremos que a y b son congruentes módulo n (lo escribiremos $a \equiv b \pmod{n}$, $a \equiv b\ (n)$ o simplemente $a = b$ cuando estemos sobre un módulo fijo) cuando $a - b$ sea un múltiplo de n, es decir, cuando $a - b = nt$ para algún $t \in \mathbb{Z}$.*

Denotaremos $\mathbb{Z}_n$ al conjunto $\{0, 1, 2, \cdots, n-1\}$ con las operaciones definidas *salvo múltiplos de n.*

Proposición 2. *Para cualquier entero positivo n y cualquier a en $\mathbb{Z}$, existe un elemento $r \in \{0, 1, \cdots, n-1\}$ tal que $a \equiv r \pmod{n}$. Esto garantiza que el resultado de cualquier operación aritmética en $\mathbb{Z}_n$ se podrá poner de nuevo en $\mathbb{Z}_n$ eligiendo este elemento r que llamaremos reducido módulo n correspondiente a a.*

Demostración. Si dividimos a entre n tenemos un cociente q y un resto r enteros. El resto será un número menor que el divisor, es decir, entre 0 y $n-1$, y se cumplirá la relación fundamental de que dividendo es igual a divisor por cociente más resto. Es decir,

$$a = nq + r$$

por lo tanto $a - r = nq$ que es un múltiplo de n y por lo tanto $a \equiv r \pmod{n}$. □

Al hacer operaciones en aritmética modular, no es necesario estar reduciendo constantemente al elemento más reducido posible. No hay ningún problema si se suman o restan múltiplos del módulo en cualquier operación intermedia. Esto permite una mayor agilidad a la hora de operar.

2. Erratas

(No detectadas)

3. Ejercicios

Conviene hacer operaciones y reducirlas módulo n para distintos módulos y distintas formas de reducir, por ejemplo, si queremos calcular módulo 5 la operación $3 \cdot 4 - 3$ podemos hacer:

$$3 \cdot 4 - 3 = 12 - 3 = 9 \equiv 4 \pmod{5}$$

o también

$$3 \cdot 4 - 3 = 12 - 3 \equiv 2 - 3 = -1 \equiv 4 \pmod{5}$$

Para practicar, utilizando varios módulos pequeños como el 2, 3 ó 5 realiza operaciones combinadas de sumas y productos haciendo las reducciones en lugares diferentes y comprobando que el resultado es el mismo.