Fundamentos de Matemáticas.

Nota sobre relaciones de congruencia

Fijado un número $n \neq 0$ de $\mathbb{Z}$, se dice que $x, y \in \mathbb{Z}$ son congruentes módulo n,y se escribe $x \approx y$, si $x - y$ es divisible por n. La relación "x congruente con y módulo n" es una relación de equivalencia en $\mathbb{Z}$ (cumple las propiedades reflexiva, simétrica y transitiva), y por tanto determina en $\mathbb{Z}$ una partición, cuyos elementos, es decir, las clases de equivalencia, constituyen el conjunto cociente $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. Es obvio que al dividir por n cualquier elemento perteneciente a una determinada clase, el resto de la división es el mismo y por tanto podemos representar la clase por el resto. Por ejemplo, si $n = 4$, la relación define en $\mathbb{Z}$ cuatro clases que podemos representar por $0, 1, 2, 3$.

Además es claro que si $x \approx y$ y $x' \approx y'$ (mod n), entonces $x \pm x' \approx y \pm y'$ y $xx' \approx yy'$ (mod n), entonces, si representamos por $C(x)$ la clase de equivalencia a la que pertenece x, resulta que

$$C(a) + C(b) = C(a + b) \quad \text{y} \quad C(a) \cdot C(b) = C(ab)$$

Como consecuencia de las propiedades del anillo $(\mathbb{Z}, +, \cdot)$ se obtiene que $(\mathbb{Z}/n, +, \cdot)$ es también un anillo con unidad y conmutativo.

Como ejemplo, consideremos el conjunto

$$\frac{\mathbb{Z}}{3\mathbb{Z}} = \{[0], [1], [2]\}$$

tiene tres elementos [0], [1], [2] que se pueden "identificar", cada uno, con los conjuntos de números que tienen igual resto al dividir por 3. Más específicamente como aquellos elementos cuya diferencia es multiplo de 3

- $[0] = \{3z : z \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \pm 9, \pm 12, ...\}$
- $[1] = \{3z + 1 : z \in \mathbb{Z}\} = \{\pm 1, \pm 4, \pm 7, \pm 10, \pm 13, \pm 16, ...\}$
- $[2] = \{3z + 2 : z \in \mathbb{Z}\} = \{\pm 2, \pm 5, \pm 8, \pm 11, ...\}$

Así la clase de equivalencia [0] se corresponden con aquellos números $\{0, 3, 6, 9, 12, ...\}$ que tienen resto 0 al dividir por 3. Como es una relación binaria de equivalencia [1] cualquier elemento del conjunto puede ser un representante del mismo. Es decir

$$\begin{aligned} [0] &= [3] = [6] = ... \\ [1] &= [4] = [7] = ... \end{aligned}$$

Teniendo en cuenta esto, para dicho conjunto se puede definir una operación "suma" sin más que sumar directamente los representantes

$$[m] + [n] := [m + n],$$

ya que se puede probar que la suma de dos números que tiene el mismo resto que m y n al dividir por 3 tiene necesariamente el

[1] véase curso cero

mismo resto que el número $m + n$. Un ejemplo

$$[1] + [2] = [1 + 2] = [3] = [0]$$

Lo que quiere decir que la suma de dos números que tiene resto 1 sumado por otro que tenga resto 2 al dividir por 3 da necesariamente un número que tiene resto 0 al dividir por 3. Por ejemplo 1+11 = 12.