U N C U E R P O F I N I T O E L E M E N T A L

Servio Tulio Eraso C.

Este artículo está dirigido tanto a los profesores de Secundaria como a sus estudiantes de los dos últimos años y pretende hacer comprender que la Matemática , así sea de nivel avanzado, se puede explicar en términos elementales ayudados por la intuición, de manera que despierte gusto por ella y se incline a investigar los tópicos de su interés.

El tema tiene que ver con la estructura algebráica de cuerpo, la cual, ya se contempla en los programas de Secundaria. Su interpretación sólo requiere algunas nociones de aritmética.

Empecemos por contar en base diez:

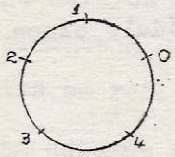
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, ...

Luego, contemos en base cinco:

1, 2, 3, 4, 10, 11, 12, 13, 14, 20, 21, 22, 23, ...

y consideremos únicamente las cifras de las unidades:

1, 2, 3, 4, 0, 1, 2, 3, 4, 0, 1, 2, 3, ...



observamos que ellas se repiten, como sucede al contar las horas en un reloj.

Por otra parte, dividamos cualquier número entero entre cinco: si la división es exacta, su residuo es cero; en caso contrario, el residuo puede ser 1, 2, 3 ó 4. Por ejemplo:

$$1475 = 295(5) + 0$$

$$241 = 48(5) + 1$$

$$372 = 74(5) + 2$$
$$-77 = (-16)(5) + 3$$
$$424 = 84(5) + 4$$

Ahora, de acuerdo al residuo obtenido organizamos los números enteros ($\mathbb{Z}$) en cinco conjuntos (infinitos) llamados clases residuales módulo cinco:

$$\overline{0} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$$
$$\overline{1} = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$$
$$\overline{2} = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$$
$$\overline{3} = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$$
$$\overline{4} = \{\ldots, -11, -6, -1, 4, 9, 14, 17, \ldots\}$$

Al observar los conjuntos anteriores, sin dificultad podemos concluír:

1. Las clases residuales no tienen elementos comunes. Es decir, son disjuntos dos a dos.
2. La reunión de todas las clases residuales es igual al conjunto de los números enteros.

Esto es, las clases residuales particionan o separan a los números enteros en células no vacías.

El conjunto de todas las clases residuales módulo cinco se denota por $\mathbb{Z}_5$:

$$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

Hecho esto, podemos construír una aritmética definiendo operaciones entre clases residuales. Para ello tomemos un representante de la clase $\overline{3}$ y otro de la clase $\overline{4}$:

$$98 \in \overline{3} \quad y \quad 98 = 19(5) + 3$$
$$64 \in \overline{4} \quad y \quad 64 = 12(5) + 4$$

Sumamos: $98 + 64 = 162$ y $162 = 32(5) + 2$

Luego, $162 \in \overline{2}$

Lo mismo sucede al tomar otros representantes de las otras clases residuales. Por lo tanto, podemos concluír que:

$$\overline{1} + \overline{2} = \overline{3};\ \overline{2} + \overline{4} = \overline{1};\ \overline{4} + \overline{4} = \overline{3};\ \overline{2} + \overline{3} = \overline{0},\ldots$$

Dicho de otra manera, la adición de clases residuales es una operación interna (binaria) y la sintetizamos en la siguiente tabla:

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$(\mathbb{Z}_5, +)$

Analicemos qué propiedades tiene esta adición:

a). La clase $\overline{0}$ es el elemento neutro de $+$, ya que para todo $\overline{x}$ en $\mathbb{Z}_5$ se cumple,

$$\overline{x} + \overline{0} = \overline{0} + \overline{x} = \overline{x}$$

(Ver primera fila y primera columna).

b). Cada elemento de $\mathbb{Z}_5$ tiene su respectivo inverso aditivo en $\mathbb{Z}_5$. En efecto, el inverso de $\overline{0}$ es $\overline{0}$; el inverso de $\overline{1}$ es $\overline{4}$; el de $\overline{2}$ es $\overline{3}$; el de $\overline{3}$ es $\overline{2}$ y el de $\overline{4}$ es $\overline{1}$.

c). La adición de clases es conmutativa, porque para todos los elementos de $\mathbb{Z}_5$ se cumple, $\overline{a} + \overline{b} = \overline{b} + \overline{a}$. (Los elementos se reflejan en la diagonal principal de la tabla).

d). La adición de clases es asociativa, pues, la suma de tres elementos de $\mathbb{Z}_5$ se puede realizar en cualquier orden sin que altere el resultado. Por ejemplo:

$$(\overline{3} + \overline{4}) + \overline{2} = \overline{2} + \overline{2} = \overline{4} = \overline{3} + \overline{1}$$
$$= \overline{3} + (\overline{4} + \overline{2})$$

$$(\overline{2} + \overline{1}) + \overline{4} = \overline{3} + \overline{4} = \overline{2} = \overline{2} + \overline{0}$$
$$= \overline{2} + (\overline{1} + \overline{4})$$

De los cuatro literales anteriores concluímos que $(\mathbb{Z}_5, +)$ es un grupo conmutativo (Abeliano).

Ahora, definamos una multiplicación de clases. Tomamos un representante de la clase $\overline{3}$ y otro de la clase $\overline{4}$:

$$43 \in \overline{3} \quad y \quad 43 = 8(5) + 3$$
$$-31 \in \overline{4} \quad y \quad -31 = (-7)(5) + 4$$

Multiplicamos: $43(-31) = -1333 = (-267)(5) + 2.$

Luego, $-1333 \in \overline{2}$.

Lo mismo ocurre con otros elementos y otras clases. Entonces:

$\overline{2} \times \overline{3} = \overline{1}$; $\overline{3} \times \overline{4} = \overline{2}$; $\overline{4} \times \overline{0} = \overline{0}$; $\overline{2} \times \overline{4} = \overline{3}$; ...

Por tanto, la multiplicación de clases residuales es una operación interna (binaria) y la resumimos en la siguiente tabla, excluyendo la clase $\overline{0}$ que anula todo:

x	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$(\mathbb{Z}_5^*, \times)$

Analizamos las propiedades de esta multiplicación:

a). La clase $\overline{1}$ es el neutro de x, pues $\overline{a} \times \overline{1} = \overline{1} \times \overline{a} = \overline{a}$ para todo $\overline{a}$ en $\mathbb{Z}_5$.
(Ver primera fila y primera columna).

b). Todo elemento no nulo de $\mathbb{Z}_5$ tiene su inverso multiplicativo en $\mathbb{Z}_5$. Así, pues, el inverso de $\overline{1}$ es $\overline{1}$; el inverso de $\overline{2}$ es $\overline{3}$; el inverso de $\overline{3}$ es $\overline{2}$ y el inverso de $\overline{4}$ es $\overline{4}$.

c). La multiplicación de clases es conmutativa, porque para todos los elementos de $\mathbb{Z}_5$ se cumple $\overline{a} \times \overline{b} = \overline{b} \times \overline{a}$.
(La tabla es simétrica con respecto a la diagonal principal)

Ejemplo: $\overline{4} \times \overline{3} = \overline{3} \times \overline{4} = \overline{2}$; $\overline{2} \times \overline{4} = \overline{4} \times \overline{2} = \overline{3}$; ...

d). La multiplicación de clases es asociativa, pues, el producto de tres elementos de $\mathbb{Z}_5$ se puede efectuar en cualquier orden y el resultado es el mismo. Es decir,

$(\bar{a} \times \bar{b}) \times \bar{c} = \bar{a} \times (\bar{b} \times \bar{c})$. Por ejemplo:

$$(\bar{2} \times \bar{3}) \times \bar{4} = \bar{1} \times \bar{4} = \bar{4} = \bar{2} \times \bar{2} = \bar{2} \times (\bar{3} \times \bar{4})$$
$$(\bar{4} \times \bar{2}) \times \bar{2} = \bar{3} \times \bar{2} = \bar{1} = \bar{4} \times \bar{4} = \bar{4} \times (\bar{2} \times \bar{2})$$

Por tanto, las clases residuales no nulas con la multiplicación forman un grupo conmutativo y se denota por $(\mathbb{Z}_5^*, \times)$.

Las dos operaciones anteriores se relacionan mediante la ley distributiva de la multiplicación con respecto a la adición:

$$\bar{a} \times (\bar{b} + \bar{c}) = (\bar{a} \times \bar{b}) + (\bar{a} \times \bar{c})$$

para todos los elementos de $\mathbb{Z}_5$. Por ejemplo:

$$\bar{3} \times (\bar{2} + \bar{4}) = \bar{3} \times \bar{1} = \bar{3} = \bar{1} + \bar{2} = (\bar{3} \times \bar{2}) + (\bar{3} \times \bar{4})$$
$$(\bar{3} + \bar{4}) \times \bar{2} = \bar{2} \times \bar{2} = \bar{4} = \bar{1} + \bar{3} = (\bar{3} \times \bar{2}) + (\bar{4} \times \bar{2})$$

De todo este desarrollo, sacamos la siguiente conclusión: los enteros módulo cinco forman un cuerpo finito, con la adición y multiplicación de clases residuales y se denota por $(\mathbb{Z}_5, +, \cdot)$.

Esta construcción se puede llevar a cabo tomando como módulo cualquier número primo (positivo). Es decir, $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo finito.

Entre las múltiples aplicaciones de los enteros módulo n está la teoría de la divisibilidad de enteros. Veamos un ejemplo concreto: Deducir una regla de divisibilidad por siete. (Lo desarrollamos en tres pasos).

1.- Todo número entero $x = a_n\, a_{n-1}\, a_{n-2} \cdots a_3\, a_2\, a_1\, a_0$ se puede expresar en términos de las potencias de diez. Por ejemplo:

$279 = 9 + 70 + 200 = 9 + 7 \times 10 + 2 \times 10^2$

$1492 = 2 + 90 + 400 + 1000 = 2 + 9 \times 10 + 4 \times 10^2 + 10^3$

$38794 = 4 + 90 + 700 + 8000 + 30000$

$= 4 + 9 \times 10 + 7 \times 10^2 + 8 \times 10^3 + 3 \times 10^4$

En general,

$$x = a_0 + a_1.10^1 + a_2.10^2 + a_3.10^3 + \ldots + a_n.10^n$$

2.- Expresamos cada potencia de 10 utilizando los residuos de dividirlas entre siete, así:

$10 = 7(1) + 3$

$10^2 = 7(14) + 2$

$10^3 = 7(142) + 6$

$10^4 = 7(1428) + 4$

$10^5 = 7(14285) + 5$

$10^6 = 7(142857) + 1$

$10^7 = 7(1428571) + 3$, etc.

3.- Como el número $x = a_n\, a_{n-1} \ldots a_3\, a_2\, a_1\, a_0$ donde cada a_i representa un dígito (de 0 a 9) volvemos a la expresión decimal dada en 1.:

$a_0 = 7 \times 0 + a_0$

$10^1 a_1 = (7 + 3)\, a_1 = 7\, a_1 + 3\, a_1$

$10^2 a_2 = (98 + 2)\, a_2 = 7(14\, a_2) + 2\, a_2$

$10^3 a_3 = (994 + 6)\, a_3 = 7(142\, a_3) + 6\, a_3$

$10^4 a_4 = (9996 + 4)\, a_4 = 7(1428\, a_4) + 4\, a_4$

$10^5 a_5 = (99995 + 5)\, a_5 = 7(14285\, a_5) + 5\, a_5$

$10^6 a_6 = (999999 + 1)\, a_6 = 7(142857\, a_6) + 1\, a_6$

$10^7 a_7 = (9999997 + 3)\, a_7 = 7(1428571\, a_7) + 3\, a_7$

etc.

Para que el número x sea divisible por siete, tanto la suma de la parte izquierda como la de la parte derecha debe ser múltiplo de siete. Es decir,

$$a_0 + 3a_1 + 2\, a_2 + 6\, a_3 + 4\, a_4 + 5\, a_5 + a_6$$

es múltiplo de siete.

EJEMPLOS.

1. Veamos si el número 7168 es divisible por 7:

   $8 + 3(6) + 2(1) + 6(7) = 70 = 7(10)$

2. El número 38794 será múltiplo de 7 ?

   $4 + 3(9) + 2(7) + 6(8) + 4(3) = 105 = 7(15)$

3. El número 2527142, no es divisible por 7:

   $2 + 3(4) + 2(1) + 6(7) + 4(2) + 5(5) + 2 = 93 \neq 7k$

   El lector halle una regla de divisibilidad por 13.

La mayoría de mis lectores se hallarán decepcionados al saber que mediante la observación común se revela el secreto de la continuidad.

R. Dedekind.

Contra la estupidez los mismos dioses pelean inútilmente

Schiller.