AMPLIACIÓN DE MATEMÁTICAS

CONGRUENCIAS DE ENTEROS.

Dado un número natural $m \in \mathbb{N}\backslash\{0\}$ sabemos (por el Teorema del Resto) que para cualquier entero $a \in \mathbb{Z}$ existe un único resto r de modo que

$$a = qm + r$$

con

$$r \in \{0, 1, 2, ..., m-1\}.$$

Así respecto de m todos los números enteros son de m " tipos" distintos (o m clases de **congruencia**). Este hecho va a permitir definir cuerpos de cardinal finito, mucho más fáciles de manejar computacionalmente que los cuerpos de números tradicionales: $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ (todos ellos infinitos).

Definición 1. *Sea $m \in \mathbb{N}\backslash\{0\}$ se dice que $a, b \in \mathbb{Z}$ son **congruentes** módulo m si*

$$a = q_1 m + r \;\; y \;\; b = q_2 m + r \;\; \textit{para algunos} \;\; q_1, q_2 \in \mathbb{Z}$$

y donde

$$0 \leq r < m.$$

*(**Notación:** escribimos $a \equiv b$ mód. m o también $aR_m b$).*

La relación definida entre dos enteros por la definición anterior tiene otra formulación equivalente.

Observación 1. *$a \equiv b$ mód. m si y solo si $m|a-b$.*

Proposición 1. *R_m es una relación de equivalencia sobre $\mathbb{Z}$.*

Demostración: La relación R_m sobre $\mathbb{Z}$ es

- **reflexiva:** ya que $m|a-a=0$, para todo $a \in \mathbb{Z}$;
- **simétrica:** ya que si $m|a-b$, también $m|b-a$, para todo $a, b \in \mathbb{Z}$;

- **transitiva:** ya que si suponemos que $a \equiv b$ mód. m y $b \equiv c$ mód. m para $a, b, c \in \mathbb{Z}$, entonces tiene que existir $0 \leq r < m$ de modo que

$$a = q_1 m + r, \quad b = q_2 m + r \quad \text{y} \quad c = q_3 m + r$$

y por tanto $a \equiv c$ mód. $m\square$

Dada la **relación** de equivalencia anterior nos fijamos en el **conjunto cociente** que produce sobre $\mathbb{Z}$.

Definición 2. *Sea $m \in \mathbb{N}\backslash\{0\}$.*

A: *Dado $a \in \mathbb{Z}$, con $a = qm + r$, notaremos por $[a]_m$ la clase de equivalencia de a respecto de la relación R_m (ser **congruente módulo** m).*

$$\begin{aligned}[a]_m &= \{x \in \mathbb{Z} \ : \ x \equiv a \ mód \, m\} \\ &= \{x \in \mathbb{Z} \ : \ x = km + r \ \ k \in \mathbb{Z}\}.\end{aligned}$$

B: *Notaremos por $\mathbb{Z}_m = \mathbb{Z}/R_m$ al **conjunto cociente** generado por la relación de equivalencia R_m, es decir*

$$\mathbb{Z}_m = \{[0]_m, [1]_m, ..., [m-1]_m\}.$$

OPERACIONES EN $\mathbb{Z}_m$.

Sobre los conjuntos cocientes $\mathbb{Z}_m$ se pueden definir una suma y un producto (llamados **suma en congruencias** y **producto en congruencias**).

Definición 3. **A:** *Se define la **suma en congruencias** sobre $\mathbb{Z}_m$ como la siguiente operación:*

$$\begin{array}{rccccc} + & : & \mathbb{Z}_m \times \mathbb{Z}_m & \to & \mathbb{Z}_m & \\ & & ([a]_m, [b]_m) & \to & [a]_m + [b]_m & = & [a+b]_m. \end{array}$$

B: *Se define el **producto en congruencias** sobre $\mathbb{Z}_m$ como la siguiente operación:*

$$\begin{array}{rccccc} \times & : & \mathbb{Z}_m \times \mathbb{Z}_m & \to & \mathbb{Z}_m & \\ & & ([a]_m, [b]_m) & \to & [a]_m[b]_m & = & [ab]_m. \end{array}$$

El siguiente resultado nos dice que las operaciones que acabamos de definir no dependen de los elementos concretos de las clase de congruencia que usamos para dar las definiciones.

Proposición 2. *Las operaciones de **suma** y **producto en congruencias** sobre $\mathbb{Z}_m$ están bien definidas.*

Demostración: Sean $a, a', b, b' \in \mathbb{Z}$ de modo que

$$a \equiv a' \text{ mód } m \text{ y } b \equiv b' \text{ mód } m.$$

Entonces

A: $[a]_m + [b]_m = [a']_m + [b']_m$, esto es así ya que

$$a + b = (q_1 m + r) + (q_2 m + s) = (q_1 + q_2)m + (r + s).$$

$$a' + b' = (q_1' m + r) + (q_2' m + s) = (q_1' + q_2')m + (r + s).$$

Luego $a + b \equiv r + s$ mód. m y $r + s \equiv a' + b'$ mód. m, luego por la propiedad transitiva se tiene que $a + b \equiv a' + b'$ mód. m. Es decir $[a + b]_m = [a' + b']_m$.

B: $[a]_m[b]_m = [a']_m[b']_m$, esto es así ya que

$$ab = (q_1 m + r)(q_2 m + s) = (q_1 q_2 + s q_1 + r q_2)m + (rs).$$

$$a'b' = (q_1' m + r)(q_2' m + s) = (q_1' q_2' + s q_1' + r q_2')m + (rs).$$

Luego $ab \equiv rs$ mód. m y $rs \equiv a'b'$ mód. m, luego por la propiedad transitiva se tiene que $ab \equiv a'b'$ mód. m. Es decir $[ab]_m = [a'b']_m \square$

Ejemplo 1. *Consideramos* $(\mathbb{Z}_4, +, \times) = (\{[0]_4, [1]_4, [2]_4, [3]_4\}, +, \times)$.

Podemos construir las **tablas** de ambas operaciones.

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

$\times$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Notación: una vez que fijamos la congruencia en la que estamos, en este ejemplo $\mathbb{Z}_4$, no escribimos $[a]_4$ ni $[a]$. Solamente a. Así, si en $\mathbb{Z}_4$ nos encontramos con el problema: $346 - 127$, lo resolveremos como $346 - 127 = 2 - 3 = 2 + 1 = 3$; donde implícitamente hemos hecho

$$\begin{array}{cc} 346 & |\underline{4} \\ 2 & 86 \end{array} \qquad\qquad \begin{array}{cc} 127 & |\underline{4} \\ 3 & 31. \end{array}$$

y además hemos "visto" en las tablas que $-3 = 1$.

Obervación: si nos fijamos en las tablas de arriba vemos que el $[0]$ y el $[1]$ son los elementos neutros de la suma y el producto, respectivamente. Mirando ahora la tabla de multiplicación de $\mathbb{Z}_4$, vemos que $[2][2] = [0]$ y que no existe ningún $[a]$ de modo que $[2][a] = [1]$. Las operaciones que acabamos de definir no tienen (siempre) las mismas propiedades que la suma y el producto a los que estamos acostumbrados.

Proposición 3. *Para $[n] \in \mathbb{Z}_m$, existe su inverso respecto de la multiplicación si y solo si $m.c.d.(n, m) = 1$.*

$$\left(\quad \exists [n]^{-1} \Leftrightarrow \exists [k] \in \mathbb{Z}_m \text{ con } [n][k] = [1] \Leftrightarrow m.c.d.(n, m) = 1 \quad \right).$$

Demostración: Si calculamos en mínimo común divisor de n y m ocurrirá que o bien

- $m.c.d.(n, m) = 1$. En este caso, por el Lema de Bezout, existen $u, v \in \mathbb{Z}$ de modo que

$$1 = un + vm \Rightarrow un = -vm + 1 \Rightarrow [u][n] = 1.$$

  Así existe $[n]^{-1} = [u]$. En otro caso tendremos que
- $m.c.d.(n, m) = r > 1$. Así podemos escribir, $n = q_1 r$ y $m = q_2 r$ con $1 \leq q_2 < m$. Luego se tiene que

$$[n][q_2] = [q_1 r q_2] = [q_1 m] = [0], \qquad \text{con} \qquad [q_2] \neq 0.$$

  Si exitiese $[n]^{-1}$, despejando en la ecuación $[n][q_2] = [0]$ tendríamos que

$$[q_2] = [n]^{-1}[0] = [0],$$

  lo cuál claramente es una contradicción $\square$

Esta proposición nos dice cuando podemos esperar que una congruencia vaya a tener inverso respecto de la multiplicíón. Además es la herramienta teórica que nos va a permitir definir y manipular la **función de Euler** que veremos más adelante.

Ejemplo 2. *¿Existe el inverso de 6 en $\mathbb{Z}_{17}$?*

En este caso, como 17 es un número primo, todo elemento no nulo de $\mathbb{Z}_{17}$ tiene inverso. Si $a \in \mathbb{N}\backslash\{0\}$, entonces $m.c.d.(a, 17) = 1$; en particular lo anterior es cierto para 6.

Ahora ¿cómo calculamos $[6]^{-1}$? Para ello necesitamos el lema de Bezout y el algoritmo de Euclides. Así dividiendo

$$\begin{array}{cc|c} 17 & 6 & \underline{2} \\ 5 & & \end{array}; \qquad \begin{array}{cc|c} 6 & 5 & \underline{1} \\ 1 & & \end{array}; \qquad \begin{array}{cc|c} 5 & 1 & \underline{5} \\ 0 & & \end{array}$$

planteamos la tabla

i	0	1	2	3	4	5
r_i	17	6	5	1	0	
q_i		2	1	5		
α_i	1	0	1	-1		
β_i	0	1	-2	3		

, de la cuál se deduce que

$$1 = -17 + 3 \times 6 \Rightarrow [1]_{17} = [-17]_{17} + [3]_{17}[6]_{17} \Rightarrow [3] = [6]^{-1} \square$$

Observación 2. ***El método y las operaciones que aparecen en el ejemplo anterior son básicas, tanto en el contexto de números como en él de polinomios. Digamos que son un 50 % de los problemas que nos esperan en los próximos temas.***

Teorema 1. *Sea* $m \in \mathbb{N}\backslash\{0\}$.

A: $(\mathbb{Z}_m, +, \times)$ *es un anillo conmutativo.*

B: $(\mathbb{Z}_m, +, \times)$ *es un cuerpo si y solo si* m *es primo.*

Demostración: $(\mathbb{Z}_m, +)$ es un **grupo conmutativo**. Claro, la suma de congruencias, dada su definición, es conmutativa y asociativa. [0] es el elemento neutro y para cada $[n] \in \mathbb{Z}_m$ es claro que $[-n]$ es su opuesto.

En $(\mathbb{Z}_m, \times)$ el producto de congruencias, dada su definición, es conmutativo y asociativo. [1] es el elemento neutro.

Además es claro que tenemos la propiedad **distributiva**,

$$[n]([k] + [r]) = [n(k + r)] = [nk + nr] = [nk] + [nr] = [n][k] + [n][r].$$

Observemos que debajo de las propiedades de las operaciones en congruencias están las propiedades de la suma y el producto de enteros.

Con lo anterior podemos asegurar que $(\mathbb{Z}_m, +, \times)$ es un anillo conmutativo para todo $m \in \mathbb{N}\backslash\{0\}$.

Ahora para que $(\mathbb{Z}_m, +, \times)$ sea un **cuerpo**, se necesita que todo elemento no nulo de $(\mathbb{Z}_m, \times)$ tenga un inverso. Según la proposición anterior eso ocurre si y solo si $m.c.d.(n, m) = 1$ para todo $n \in \{1, 2, 3, ..., m-1\}$. Lo cuál es equivalente a decir que m es primo $\square$

Observación 3. *Si* m ***no*** *es primo, entonces existe* $n > 1$ *con* $n|m$ *y así* $m = qn$. *Pasando a congruencias*

$$[q][n] = [m] = [0] \qquad \textit{donde} \qquad [q] \neq 0 \qquad y \qquad [n] \neq 0.$$

Definición 4. *En un anillo* $(\mathbb{A}, +, \times)$ *donde* e *es el elemento neutro de la suma, se llaman* ***divisor de cero*** *a todo elemento* $a \in \mathbb{A}\backslash\{e\}$ *de modo que existe otro elemento* $b \in \mathbb{A}\backslash\{e\}$ *para los cuáles*

$$a \times b = e.$$

Un anillo $(\mathbb{A}, +, \times)$ *se llama* ***dominio de integridad*** *si* ***no*** *tiene divisores de cero.*

En el tema de **anillos** retomaremos estas definiciones. Parece claro que siempre es mejor trabajar en sitios donde no haya divisores de cero.

Ejemplo 3.

- $(\mathbb{Z}, +, \times)$ ***no*** *tiene divisores de cero. Es el ejemplo típico (junto a los anillos de polinomios) de dominio de integridad.*
- *Si* m ***no*** *es primo, entonces* $(\mathbb{Z}_m, +, \times)$ ***tiene*** *divisores de cero. Es el ejemplo típico de anillo con divisores de cero. Estos anillos no son muy interesantes para trabajar con ellos.*
- *Si* p *es* ***primo****, entonces* $(\mathbb{Z}_p, +, \times)$ *es un* ***cuerpo*** *que es algo más que ser dominio de integridad. Claro, en este caso tampoco hay divisores de cero.*

Observación 4. $\mathbb{Z}$ ***no*** *es un cuerpo. No todos los elementos de* $\mathbb{Z}$ *(de hecho ninguno salvo el* 1 *y el* -1*) tiene inverso respecto del producto.*

Las **fracciones** de elementos de $\mathbb{Z}$ permiten construir el cuerpo de los números racionales $\mathbb{Q}$, que incluye a los números enteros. Si $(\mathbb{A}, +, \times)$ es un anillos sin divisores de cero (es decir lo que llamos un **dominio de integridad**), se pueden definir las fracciones de elementos de $\mathbb{A}$ (de forma análoga como se hace para construir $\mathbb{Q}$)para crear un cuerpo de fracciones, que es un cuerpo que contiene a $\mathbb{A}$. Aunque utilizaremos esta técnica con los anillos de polinomios, no es el camino que más no va a interesar.

Observación 5. *Otra forma de "superar" que* $\mathbb{Z}$ *no es un cuerpo es considerando* $(\mathbb{Z}_p, +, \times)$ *con* p *primo. Este conjunto, como sabemos, es un cuerpo.* ***No*** *podemos decir que* $\mathbb{Z} \subset \mathbb{Z}_p$ *(como si pasa con* $\mathbb{Z} \subset \mathbb{Q}$*), pero en cambio* $\mathbb{Z}_p$ *es finito, solo tiene* p *elementos. Esta ventaja la veremos al estudiar* ***cuerpos finitos****.*

Ejercicio 1. *Hay que resolver la* ***ecuación en congruencias***

$$5x \equiv 17 \qquad \textit{mód.} \qquad 19.$$

Como 19 es primo, existe $[5]^{-1} \in \mathbb{Z}_{19}$, y así $x \equiv [5]^{-1}17$ mód. 19. Haciendo la tabla de multiplicar de $\mathbb{Z}_{19}$ o buscando una identidad de Bezout $(1 = u19 + v5)$, vemos que $[4][5] = [1]$, y así

$$x \equiv 4 \times 17 = 68 \equiv 11 \qquad \text{mód.} \qquad 19.$$

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
E-mail address: Cesar_Ruiz@mat.ucm.es