Aritmética modular

La aritmética modular es una forma de representar números para que su valor nunca exceda un cierto límite, llamado módulo. [1]

Cuando se cuenta en aritmética modular, si alcanza el módulo, se restablece a 0 y comienza se a contar nuevamente, por lo que, por ejemplo, el número 18 en módulo 12 sería 6: cuenta hasta 12, restablece a 0 y luego cuenta los 6 restantes.

Es común introducir estas ideas utilizando el ejemplo del módulo 12 ya que todos estamos familiarizados con la que a veces se le llama aritmética de reloj, aunque es un concepto que aparece en varias situaciones bastante diferentes (como mencionaremos más adelante ó como ya vimos por ejemplo con los ángulos y otras equivalencias).

En su obra *Disquisitiones Arithmeticae*, publicada en el a no 1801, **Gauss** introdujo el concepto de congruencia.

Definición 0.1. *Dados los enteros a, b y m, se dice que* a es congruente con b módulo m *y se escribe* $a \equiv b \pmod{m}$ *(ó* $a \equiv_m b$ *ó* $a \equiv b\ (m)$ *) si y sólo si* $m|a-b$*, es decir, existe* $k \in Z$ *tal que* $a - b = k.m$

Ejemplo 0.2. $4 \equiv 10\ (3)$ *pues* $3|4-10$*, ya que existe* -2 *tal que* $4 - 10 = -6 = -2 \cdot 3$

[1] puede que a muchos le resulte conocido el cálculo del módulo y su símbolo % , que se utiliza comúnmente para producir el resto de una división, pero también puede ser se utiliza para comprobar si un número es un factor de otro, porque si lo es, el resto debe ser cero.

Proposición 0.3. *La relación de congruencia módulo m es una relación de equivalencia*

Demotración: Para mostrar que la congruencia es una relación de equivalencia tenemos que probar que es reflexiva, simétrica y transitiva.

Tenemos: *a es congruente con b módulo m* , ó $a \equiv_m b$ si y sólo si $m|a-b$, entonces,

- $\equiv_m$ es reflexiva ya que para a entero vale que $m|a-a$ pues $a-a=0.m$
- $\equiv_m$ es simétrica.

  Supongamos que $a \equiv_m b$, entonces m divide a $a-b$ y existe k entero tal que $a-b=k.m$, luego existe $-k$ tal que $b-a=-(a-b)=-(k.m)=(-k).m$ y por lo tanto $m|b-a$ y $b \equiv_m a$
- $\equiv_m$ es transitiva: esto es, si $a \equiv_m b$ y $b \equiv_m c$ entonces $a \equiv_m c$

  Supongamos que $a \equiv_m b$ entonces $m|a-b$, existe k entero tal que $a-b=km$,

  por otro lado $b \equiv_m c$ entonces $m|b-c$, existe h entero tal que $b-c=hm$,

  luego $a-c=a+(-b+b)-c=(a-b)+(b-c)=km+hm=(k+h)m$, y existe un entero $t=k+h$ tal que $a-c=tm$ y así m divide a $a-c$ y de esa forma tenemos que $a \equiv_m c$ como queríamos probar.

Por ser la congruencia una relación de equivalencia en $\mathbb{Z}$, determina una partición del conjunto de los números enteros en *clases de equivalencia* que se denominan *clases de congruencia módulo m* .

La clase de congruencia módulo m de un número x será el conjunto $\overline{x}=\{y \in \mathbb{Z} : y \equiv_m x\}$

Esto nos permite agrupar a los enteros en familias disjuntas de manera que dos números son congruentes módulo m si y sólo si están en la misma clase de equivalencia.

Esta partición de $\mathbb{Z}$ inducida por la congruencia módulo m es lo que nos determina el conjunto cociente $\mathbb{Z}m=\mathbb{Z}_m=\mathbb{Z}/\equiv_m$ que estaremos estudiando.

Observación 0.4. *Dos números enteros pertenecen a la misma clase de equivalencia si y sólo si son congruentes módulo m.*
Supongamos que a y b pertenecen a la "clase del x", entonces $a \equiv_m x$ y $b \equiv_m x$. Como la congruencia es una relación simétrica y transitiva tenemos que $a \equiv_m b$.
Por otro lado, si $a \equiv_m b$ es claro que ambos pertenecen a la misma clase de equivalencia.

Proposición 0.5. *Todo entero es **congruente módulo** m con su **resto** en la división por m*

Demostración:

Supongamos que $x \equiv_m y$, sabemos que esto equivale a decir que existe k entero tal que $x - y = km$, entonces podemos escribir $x = km + y$.
Como antes dijimos que dos enteros son congruentes si pertenecen a la misma clase podemos con ésto describir las clases de la siguiente forma:
$\overline{x} = \{y : y \equiv_m x\} = \{y : x = km + y\} = \{y : y = x + k'm\} = \{y : y = x, y = x + 1, y = x + 2.....\}$

Ejemplos 0.6. *1. Sabemos que $x \equiv_3 y$ si y sólo si $x - y = k \cdot 3$.*

Ahora tomemos por ejemplo al 2, como $y \equiv_3 2$ es lo mismo que $y - 2 = k \cdot 3$ entonces vale $y = k \cdot 3 + 2$ (todos los puntos de "esa recta")

$$\bar{2} = \{y \in Z : y \equiv_3 2\} = \{2, 5, 8, 11, \cdots\}$$

2. Veamos la congruencia módulo 2, esto es $x \equiv_2 y$ si y sólo si $x - y = 2 \cdot m$

Tomemos al 1, Como $1 \equiv y(2)$ es lo mismo que $y - 1 = k \cdot 2$ entonces vale $y = k \cdot 2 + 1$

$$\bar{1} = \{y \in Z : 1 \equiv_2 y\} = \{1, 3, 5, 7, 9, 11, \cdots\}$$

$$\bar{0} = \{y \in Z : 0 \equiv_2 y\} = \{0, 2, 4, 6, 8, 10, \cdots\}$$

Luego, $Z/\equiv_2 = \{\bar{0}, \bar{1}\}$

"Partimos" el conjunto de los números enteros en dos clases, la del $\bar{0}$ y la del $\bar{1}$, es decir, los números que tienen resto 0 cuando se los divide por 2, o resto 1.
*Esto es, **los números pares y los impares**.*

Proposición 0.7. *Dos enteros son congruentes módulo m si y sólo si los respectivos restos en su división por m son iguales.*

Demostración:

Supongamos que x e y son dos enteros congruentes módulo m y probemos que tienen el mismo resto en la división por m.

Por el algoritmo de la división, existen (y son únicos) cociente y resto enteros tales que :

$x = k_1 m + r_1$ con $0 \leq r_1 < m$

$y = k_2 m + r_2$ con $0 \leq r_2 < m$ (Observemos que $|r_1 - r_2| < m$)

Luego, $x - y = (k_1 m + r_1) - (k_2 m + r_2) = (k_1 m - k_2 m) + (r_1 - r_2) = (k_1 - k_2)m + (r_1 - r_2)$

Y como $x \equiv_m y$, existe un entero k tal que $x - y = km$, concluimos que debe ser $r_1 - r_2 = 0$ y por lo tanto $r_1 = r_2$.

Ahora supongamos que los restos en la división por m coinciden y veremos que $x \equiv_m y$.

Otra vez usando el algoritmo de la división existen k_1, k_2, r enteros tales que :

$$x = k_1 m + r$$

$$y = k_2 m + r$$

Así, $x - y = (k_1 m + r) - (k_2 m + r) = (k_1 m - k_2 m) + (r - r) = (k_1 - k_2)m = km$

mostrando que $m|x - y$ y por lo tanto, $x \equiv_m y$.

Ejemplo 0.8. *Sea $m = 5$, vemos que $7 \equiv_5 42$ ya que ambos tienen resto 2 en la división por 5 (de hecho ambos son congruentes con 2)*

Todo entero es congruente con su resto en la división por m, $x \equiv_m r$, ya que por el algoritmo de la división para cualquier entero x existe y es único el resto r en la división por m

También sabemos que dos enteros congruentes pertenecen a la misma clase de equivalencia, y por lo tanto las clases serán iguales, $\bar{x} = \bar{r}$.

Por las propiedades y características de la división entera, tenemos que hay m posibles restos en la división por m. Estos son, 0, ..., $m - 1$.

De esta forma vemos que habrá m clases de equivalencia o congruencia.

Teorema 0.9. *Sea* $m \in N$,$\mathbb{Z}m = \mathbb{Z}_m = \mathbb{Z}/ \equiv_m$, *el conjunto cociente, tiene* m *clases de equivalencias.*

1 Aritmética en $\mathbb{Z}_m$

Dado $m \in Z$, definiremos la suma y el producto entre los elementos de $\mathbb{Z}_m$, es decir entre las clases de equivalencia módulo m.

Esta definición no dependerá del representante elegido y así podremos sumar y multiplicar clases de equivalencias y el resultado será un representante de la misma clase (es decir, las operaciones estarán bien definidas).

La relación de congruencia es *compatible* con la suma y el producto.

Dados $a, b, c, d \in Z$ tales que $a \equiv_m b$ y $c \equiv_m d$. Entonces se cumple que:

- $a + c \equiv_m b + d$
- $a \cdot c \equiv_m b \cdot d$

Probemos la compatibilidad:

Sabemos que $a - b = km$ y $c - d = hm$ por ser congruentes módulo m por hipótesis general. Sumando ambos miembros: $\underbrace{(a-b)+(c-d)}_{(a+c)-(b+d)} = km + hm = \underbrace{(k+h)}_{\in Z} m$

Con lo cual queda demostrado que $m|(a+c)-(b+d)$ y por lo tanto $a + c \equiv_m b + d$

Ahora veamos que el producto está bien definido. Al igual que con la suma tenemos que $a - b = km$ y $c - d = hm$ y queremos llegar a $ac - bd = rm$ ya que esto significa que m divide a la diferencia $ac - bd$ y por lo tanto $ac \equiv_m bd$

Multipliquemos ambos miembros de $a - b = km$ por c, $ca - cb = ckm$,
y ambos miembros de $c - d = hm$ por b, $bc - bd = bhm$

Sumando adecuadamente y utilizando las propiedades conmutativa y asociativa del producto de enteros nos queda:

$$\underbrace{(ca-cb)+(bc-bd)}_{ac-bd} = ckm + bhm = \underbrace{(ck+bh)}_{\in Z} m$$

1.1 Operaciones en $\mathbb{Z}_m$

Ya vimos que la suma y el producto son compatibles con la congruencia módulo m, ahora podemos definir las operaciones entre clases y basando esa definición en la suma y producto de enteros *heredará* varias propiedades.

Suma: $\overline{x} + \overline{y} = \overline{x + y}$

La suma tiene las siguientes propiedades:

- Asociatividad
- Conmutatividad
- Existencia del neutro
- Todo elemento tiene opuesto

Producto: $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$

El producto tiene las siguientes propiedades:

- Asociatividad
- Conmutatividad
- Existencia del neutro
- El producto se distribuye en la suma

Reiteramos que éstas propiedades son válidas gracias a la definición de las operaciones entre clases basadas en la suma y el producto de enteros.

Veamos, como ejemplo solamente, que vale la propiedad distributiva del producto en la suma:

Queremos probar que : $\overline{x} \cdot (\overline{y} + \overline{z}) = \overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z}$,

$$\overline{x} \cdot (\overline{y} + \overline{z}) = \overline{x} \cdot (\overline{y + z}) = \overline{x \cdot (y + z)} = \overline{xy + xz} = \overline{xy} + \overline{xz} = \overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z}$$

Tablas de operaciones

Sea $Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. Veamos las tablas de la suma y el producto:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$*$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Es fácil ver desde la tabla que el opuesto del $\bar{1}$es el $\bar{2}$, (y obviamente el opuesto del $\bar{2}$ es el $\bar{1}$), el inverso del $\bar{2}$ es el mismo; y que *dos más dos es uno y no cuatro...*

1.1.1 Elementos invertibles

Igual a lo que ocurre en $\mathbb{Z}$, no todos los elementos tendrán opuesto para el producto.

Definición 1.1. *Dado $\bar{a} \in Z_m$ no nulo, decimos que $\bar{a}$ es **divisor de 0** si: existe $\bar{b} \in Z_m, \neq 0$ tal que $\bar{a} \cdot \bar{b} = \bar{0}$*

Los divisores de cero son elementos no nulos (distintos del elemento neutro) tal que su producto por otro elemento no nulo da como resultado el elemento neutro.

Definición 1.2. *Dado $\bar{a} \in Z_m$, decimos que $\bar{a}$ es **invertible** (o divisor de la unidad), si: existe $\bar{c} \in Z_m$ tal que $\bar{a} \cdot \bar{c} = \bar{1}$*

Teorema 1.3. *Sea $\bar{a} \in Z_m$, $\bar{a}$ es invertible si y sólo si $(a, m) = 1$*

Demostración:

Supongamos primero que $\bar{a} \in Z_m$ es invertible, o sea, existe $\bar{c} \in Z_m$ tal que $\bar{a} \cdot \bar{c} = \bar{1}$, y esto quiere decir que $ac \equiv_m 1$, entonces $ac - 1 = m.k$ para algún k entero, o lo que es lo mismo, $ac - km = 1$

Luego, como (a, m) dividirá a cualquier combinación lineal entre a y m, $(a, m)|1$ y por lo tanto $(a, m) = 1$

Ahora pensemos que $(a, m) = 1$, entonces (usando Bezaut) $1 = sa + rm$ para s, r enteros, luego $\bar{1} = \overline{sa + rm} = \overline{sa} + \overline{rm} = \bar{s}\bar{a} + \bar{r}\bar{m} = \bar{s}\bar{a} + \bar{r}\bar{0} = \bar{s}\bar{a}$, mostrando que existe $\bar{s} \in Z_m$ que hace invertible a $\bar{a}$

Corolario 1.4. *Si $m \in Z$ es primo, Z_m es un cuerpo*

Teorema 1.5. *Dado $a \in Z_m$, a es invertible si y sólo si a NO es divisor de 0*

Ahora veamos otro resultado relacionado con las potencias de elementos de Z_m conocido como el *Pequeño teorema de Fermat*[2]

Teorema 1.6. *Si p primo entonces $\overline{a}^p \equiv_p \overline{a}$. En particular, si $\overline{a} \neq \overline{0}$ se tiene que $\overline{a}^{p-1} \equiv_p \overline{1}$*

Demostración:

Primero supongamos que $\overline{a} \equiv_p \overline{0}$, luego $\overline{a}^p \equiv_p \overline{0}^p \equiv_p \overline{0} \equiv \overline{a}$

Ahora suponemos que $\overline{a} \neq \overline{0}$, entonces $\overline{a}$ es invertible! . Vamos a probar que para p primo entonces $\overline{a}^{p-1} \equiv_p \overline{1}$ (a partir de esto el otro resultado es inmediato)

Recordemos que $Z_p = \left\{\overline{0}, \overline{1}, \cdots, \overline{p-1}\right\}$ donde cada elemento es una clase única (y no tiene elementos en común con otras clases)

Multiplicamos $\overline{a}$ por cada una de las clases de Z_p, el resultado será una clase, un elemento de Z_p, observemos que como $\overline{a}$ es invertible al multiplicarlo por diferentes clases obtengo resultados diferentes.

Supongamos que $\overline{a} \cdot \overline{b} \equiv_p \overline{a} \cdot \overline{c}$, multiplicamos a ambos lados por el inverso de $\overline{a}$ y llegamos a que $\overline{b} \equiv_p \overline{c}$ lo cual es un absurdo ya que todas las clases son distintas y disjuntas.

Entonces sabemos que el producto $\overline{a}$ con todas las clases de Z_p nos da una clase única, alguna de las clases de Z_p (excepto la clase del cero ya que $\overline{a}$ es invertible) y podemos escribir:

$(\overline{a} \cdot \overline{1})(\overline{a} \cdot \overline{2}) \cdots \overline{a} \cdot \overline{p-1} \equiv_p \overline{1} \cdot \overline{2} \cdots \overline{p-1}$

$(\overline{a} \cdot \overline{a} \cdots \overline{a}) \cdot (\overline{1} \cdot \overline{2}) \cdots \overline{p-1}) \equiv_p \overline{1} \cdot \overline{2} \cdots \overline{p-1}$

$\overline{a}^{p-1} \cdot \overline{1} \cdot \overline{2} \cdots \overline{p-1} \equiv_p \overline{1} \cdot \overline{2} \cdots \overline{p-1}$

y multiplicando a ambos lados por los inversos (ya que como p es primo todos los elementos de Z_p son invertibles) llegamos a que $\overline{a}^{p-1} \equiv_p \overline{1}$

Definición 1.7. *La función ϕ, llamada **función de Euler** , es tal que a cada número natural m le asocia el número $\phi(m)$ de elementos invertibles de Z_m*

Teorema 1.8. ***Teorema de Euler***

Sean a y m enteros tales que $a, m) = 1$, entonces $\overline{a}^{\phi(m)} \equiv_m \overline{1}$

[2]Se lo conoce con este nombre simplemente para distinguirlo del *Ultimo Teorema de Fermat*, una conjetura que fue finalmente resuelta en 1995. El teorema que vamos a ver fue comunicado sin demostración por Fermat en 1640 y fue Euler quien en 1736 publicó la primera demostración