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 año 1801, **Gauss** introdujo el concepto de congruencia, que estudiamos anteriormente, para trabajar con las clases de equivalencia de esta relación.

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* .

[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.

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.

Ejemplos 0.1. *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****.*

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

Teorema 0.2. *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: $\overline{x} \cdot \overline{y} = \overline{x} \cdot \overline{y}$

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.
fORMAN UN ANILLO

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

2 Aplicaciones a la criptografía

Una de las aplicaciones más interesantes de la Aritmética Modular ocurre en la Criptografía, en la que se utilizan las distintas operaciones, con el objeto de cifrar información.

En esta sección describiremos de manera muy simple con ejemplos (y desde la matemática) cómo se pueden usar algunos conceptos de Aritmética Modular en el cifrado de datos. En la práctica, que un programa de criptografía sea seguro o no, no depende sólo del algoritmo matemático que emplea, sino a su implementación (para mayor información aconsejamos cursar materias optativas como *Introducción a la Ciberseguridad*, etc.

Algunos ejemplos de Criptosistemas son el Cifrado César, que es que una aplicación de la adición modular, el algoritmo de Diffie-Hellman y el Criptosistema RSA que para su implementación requiere los Teorema de Euler y Fermat.

2.1 Cifrado de César

El cifrado de César es un sistema clásico que no requiere el uso de computadoras para ser implementado. Recibe este nombre debido a que Julio César usaba esta técnica para comunicarse con sus generales, es una forma de cifrado sencilla pero también es fácil de encontrar el *desciframiento*.
Es un tipo de cifrado por sustitución en el que una letra de un texto es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D(situada 3 lugares más abajo o a la derecha de la A, depende de como organicemos el alfabeto), la B sería reemplazada por la E, y así siguiendo.

Vamos con un ejemplo, tenemos dos funciones una que encriptará ($e_k(x) \equiv_m x + k$) y otra que descifrará el enigma ($d_k(x) \equiv_m x - k$) y pensemos en el alfabeto español de 27 letras.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Suponiendo que nos corremos 3 lugares (como el cifrado original de César), las funciones nos quedarán:

$e_3(x) \equiv_{27} x + 3$ y $d_3(x) \equiv_{27} x - 3$

El texto "JULIOCESAR" se cifra como una cadena de enteros, *9 21 11 8 15 2 4 19 0 18*

Ahora adicionamos 3 y obtenemos la cadena: *12 24 14 11 18 5 7 22 3 21*
(siempre en módulo 27, aunque con un texto tan corto y un número tan bajo no se nota demasiado que tomamos módulo)

Por último volvemos al cuadro del alfabeto y escribimos el texto cifrado "MXÑLRFHVDU"

En la época de Julio César, si sus enemigos encontraban un mensaje cifrado tenían que probar 26 cambios de letras para asegurarse de descifrar el mensaje, sólo un cambio sería el correcto. Este enfoque se denomina método de *fuerza bruta* . Implica probar todas las claves posibles hasta encontrar el enfoque correcto.

2.2 El cifrado RSA

El sistema criptográfico RSA (llamado así por sus creadores, Rivest, Shamir y Adleman) es un sistema de cifrado asimétrico. Se publicó en 1977 y sigue siendo la base de muchos esquemas de cifrado en la actualidad.
Este Criptosistema es una aplicación de los Teoremas de Euler y Fermat

Veamos como funciona el algoritmo,

Aquí está el algoritmo de generación de claves públicas:

1. Eligir 2 números primos (muy grandes), p y q
2. Calcular el módulo r donde $r = p \cdot q$ (esto es fácil de calcular, pero puede ser difícil de revertir)
   (Utilizaremos luego este módulo en el proceso de encriptación y desencriptación)
3. Calcular la función de Euler $\phi = (p-1) \cdot (q-1)$
4. Eligir un número mayor que 1 y menor que ϕ que sea coprimo con ϕ (es decir cualquier número menor (si se elige mayor se vuelve a ajustar por el módulo) que ϕ que no tenga divisor común con él).
   Llamar a este número e
5. e es el exponente público
   Las claves públicas para RSA vienen en un par: una mitad es el módulo RSA y la otra un exponente. Por ejemplo, si el módulo RSA r fuera 183 y el exponente e fuera 97, la clave quedaría así: $\{183, 97\}$.
6. El exponente privado d es la inversa de e módulo ϕ (es decir, $e \cdot d \equiv_\phi 1$
7. Producir la clave privada encontrando la inversa modular de la pública utilizando ϕ como módulo

Podemos hacer públicos e y r . Si p y q son lo suficientemente grandes, no se pueden *adivinar* utilizando r, lo que significa que nadie más tiene la capacidad de encontrar d usando e y r.

Para encriptar un mensaje $\boldsymbol{m}$ usando RSA, eleve su mensaje a la potencia e (su exponente público) y aplique su módulo r, por lo que el texto cifrado $\boldsymbol{c}$ se calcula así: $c \equiv_r m^e$

Para descifrar un texto cifrado, se lo eleva a la potencia d (su exponente privado) y se aplica el módulo r: $m \equiv_r c^d$

Tratemos de clarificar el algoritmo con un ejemplo repitiendo los pasos de la generación de claves, cifrado y descifrado utilizando números pequeños:

Generación de claves:

1. El primer paso es elegir dos números primos. Por ejemplo 11 y 19 [3]
2. calcular el módulo RSA: $r = p \cdot q = 11 \cdot 19 = 209$
3. calculamos $\phi = (p-1) \cdot (q-1) = 10 \cdot 18 = 180$
4. Elegir un número que es mayor que 1 y menor que 180 que sea coprimo con 180, por ejemplo 13.
   (13 es el exponente público y $\{13, 209\}$ es la clave pública)
5. El último paso es determinar la clave privada d.
   d es tal que $e \cdot d \equiv_\phi 1$, tengo que encontrar el inverso modular de $e = 13$ módulo $\phi = 180$

   Resolvemos usando el algoritmo de Euclides extendido (o calculadoras para inversos modulares) y obtenemos que $d = 97$

[3] Recuerde, si p y q son lo suficientemente grandes, es computacionalmente imposible calcular simplemente por conocer su producto r

El algoritmo de generación de claves dio como resultado el siguiente conjunto de números:

- $p = 11$ y $q = 19$ *hay que mantenerlas privadas*
- $r = 209$ *se puede hacer pública*
- $\phi = 180$ *mantener privada*
- $e = 13$ *hacer pública*
- $d = 97$ *mantener privada*

Cifrado *:* Encriptemos el número 14.Para hacer esto, lo elevo al valor de la clave pública e y lo reduzco módulo r:

$$c \equiv_{209} 14^{13} = 192$$

Descifrado**:** Para descifrar c, lo elevo al valor de la clave privada y, nuevamente, lo aplico el módulo:

$$m \equiv_{209} c^{97} \equiv_{209} 192^{97} = 14$$