0214.00

1

Aritmética Modular

3 487002 140007

1. Introducción

En este tema veremos el concepto de congruencia módulo n, así como los anillos de restos modulares y su estructura. Calcularemos inversos y resolveremos sencillas ecuaciones en congruencias.

2. Congruencias

Sea n un número entero positivo. Dados dos números a y b, diremos que son congruentes módulo n, y lo representaremos $a \equiv b(n)$ si la diferencia $a - b$ es un múltiplo de n, es decir, existe $t \in \mathbb{Z}$ tal que $a - b = nt$.

Pensemos por ejemplo en el caso $n = 2$, dos números a y b son congruentes módulo 2 si su diferencia es un múltiplo de 2, es decir, un número par. Es inmediato ver que esta relación nos divide el conjunto de todos los números en dos grupos, los pares (todos los números pares son congruentes módulo 2 entre sí) y los impares (a los que le pasa lo mismo). Podemos establecer un número par y uno impar para representar a toda la clase, por ejemplo 0 y 1. Con esto todos los números pares se pueden identificar con los números congruentes con 0 y los impares con los congruentes con 1.

La relación de congruencia es muy útil para representar situaciones cíclicas y con valores discretos. Supongamos por ejemplo un reloj que marca las horas y la congruencia módulo 12. Cuando llegamos a las 12 es como si estuviéramos en el 0 de nuevo, las 13 es lo mismo que la 1 porque $1 - 13 = -12$ que es un múltiplo de 12. Lo mismo sucede al superar la hora número 24. La hora 25 marcaría de nuevo la 1.

Dado un número a cualquiera, podemos hacer la división de a entre n y obtener un resto r que estará entre 0 y $n-1$, además cumplirá que $a = qn + r$ y por lo tanto $a - r$ será un múltiplo de n con lo que $a \equiv r(n)$. Esto prueba que todo número es congruente con alguno de entre los que hay en $\{0, 1, \cdots, n-1\}$. Además es fácil ver que dos de ellos que sean distintos no pueden ser congruentes entre sí, porque su diferencia siempre sería más pequeña que n y no podría ser un múltiplo de n a no ser que fuera 0.

La relación de congruencia módulo n satisface unas propiedades de compatibilidad con la suma y con el producto que se pueden enunciar así: Si $a \equiv a'(n)$ y $b \equiv b'(n)$ entonces $a + b \equiv a' + b'(n)$ y $a \cdot b \equiv a' \cdot b'(n)$. Cuando tenemos que hacer una serie de operaciones aritméticas sucesivas y lo único que nos interesa es con qué número es congruente el resultado final, podemos cambiar en cualquier momento un número por otro que

sea congruente con él y el resultado final no nos cambiará. Esto nos permite simplificar resultados parciales.

Por ejemplo, supongamos que queremos calcular $3^8(5)$. Podemo calcular el resultado total $3^8 = 6561$ y luego reducirlo diciendo que $6561 \equiv 1(5)$, pero también podemos hacer $3^8 = (3^2)^4 = 9^4$, pero como $9 \equiv -1(5)$, podemo decir que $9^4 \equiv (-1)^4 = 1(5)$. De esta forma hemos calculado el resultado prácticamente sin ninguna operación.

3. Los anillos $\mathbb{Z}_n$

Podemos definir el anillo $\mathbb{Z}_n$ como el conjunto $\{0, 1, \cdots, n-1\}$ junto con las operaciones de suma y producto definidas del siguiente modo. Dados dos números de $\mathbb{Z}_n$, hacemos la operación de suma y producto ordinaria, y si el resultado se sale del rango $\{0, 1, \cdots, n-1\}$ entonces calculamos el elemento que está dentro de rango que es congruente con el resultado módulo n, y ese será el resultado en $\mathbb{Z}_n$.

Por ejemplo, las tablas de sumar y multiplicar en $\mathbb{Z}_5$ son las siguientes:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Cuando estamos en un anillo del tipo $\mathbb{Z}_n$, podemos definir también los inversos de los números aditivos y multiplicativos. Si a es un elemento de $\mathbb{Z}_n$, el opuesto de a es el elemento que sumado con a nos da 0 en $\mathbb{Z}_n$. Este elemento lo denotaremos $-a$. Por ejemplo, si miramos la tabla de sumar en $\mathbb{Z}_5$, el elemento que sumado con el 2 nos da el 0 es el 3, por lo tanto podemos decir que $-2 = 3$ en $\mathbb{Z}_5$. Fijémonos que esta es precisamente la misma relación de congruencia módulo 5.

Para los inversos multiplicativos pasa algo parecido. El elemento que podríamos llamar $1/4$ ó 4^{-1} en $\mathbb{Z}_5$ es el elemento que multiplicado por 4 nos da 1 en $\mathbb{Z}_5$, que en este caso es el mismo 4 porque $4 \cdot 4 = 1$ en $\mathbb{Z}_5$. Podemos calcular todos los inversos mirando la tabla $1^{-1} = 1, 2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4$. En estos conjuntos se cumplen todas las propiedades aritméticas habituales con esta notación.

4. Inversos Modulares

Cuando estamos en módulos pequeños es posible calcular inversos haciendo toda la tabla de multilicar y mirando simplemente cual es el elemento que multiplicado por el nuestro nos da 1. Sin embargo cuando el módulo es grande, este método es muy costoso, pero podemos utilizar otro método que es similar al del cálculo de máximo común divisor extendido y que nos permite resolver el problema.

Supongamos que tenemos que calcular el inverso de 72 módulo 121, entonces podemos calcular los coeficientes u y v que nos proporcionan el máximo común divisor de estos dos números como combinación de ellos. Como el máximo común divisor es 1, tenemos que $121u + 72v = 1$ y por lo tanto $72 \cdot v \equiv 1(121)$ y por lo tanto v el el inverso que estamos buscando. Si hacemos las cuentas obtenemos lo siguiente:

a	b	r	v	t	q
121	72	49	0	1	1
72	49	23	1	-1	1
49	23	3	-1	2	2
23	3	2	2	-5	7
3	2	1	-5	37	1
2	1	0	37	-42	2
1	0		-42		

Esta tabla nos proporciona el coeficiente v que es el que buscamos y nos confirma que el máximo común divisor es 1. El resultado v que nos ha salido es -42 que si queresmos meter dentro del rango $\{0, 1, \cdots, 120\}$ es $-42 + 121 = 79$. Si comprobamos el resultado tenemos que

$$79 \cdot 72 = 5688 = 47 \cdot 121 + 1 \equiv 1(121)$$

Este método nos ha permitido calcular el inverso modular de a módulo n siempre que el máximo común divisor de a y n sea 1, pero se puede

probar que ese es el único caso posible. Un número a tiene inverso módulo n si y sólo si $mcd(n, a) = 1$.

Un ejemplo de un elemento que no tiene inverso módulo n es el 0 (el 0 nunca tiene inverso), pero por ejemplo en $\mathbb{Z}_6$, el 2 no tiene inverso porque si probamos todos los productos posibles, nunca encontraremos el 1 vemámoslo: $2 \cdot 0 = 0$, $2 \cdot 1 = 2$, $2 \cdot 2 = 4$, $2 \cdot 3 = 0$, $2 \cdot 4 = 2$, $2 \cdot 5 = 4$).

Hay conjuntos $\mathbb{Z}_n$ en los cuales todos los elementos entre 1 y $n - 1$ tienen máximo común divisor 1 con n, concretamente esta situación se da cuando n es un número primo. En estos casos se dice que $\mathbb{Z}_n$ es un cuerpo, puesto que tiene todas las propiedades aritméticas que definen esta estructura algebraica, pero a diferencia de otros cuerpos conocidos como $\mathbb{R}$ o $\mathbb{Q}$, estos conjuntos son finitos.