Aritmética Modular I

Este documento no pretende ser un curso exhaustivo, en el mejor de los casos, únicamente puede considerarse como un conjunto de notas complementarias en alguna asignatura. Por supuesto, todo documento es susceptible de mejora, cualquier sugerencia o comunicación de error u omisión será bienvenida.

Introducción. Definiciones básicas.

En criptografía se estudian los proceso que busquen transformar un mensaje con objeto de ocultar la información contenida en él. Por supuesto, para ser útil, el proceso utilizado debe ser reversible. Una estructura algebraica que permite modelar tanto el conjunto posible de mensajes como una operación de transformación es el *grupo*.

Así, un grupo es un par $\langle G, \otimes \rangle$ donde G es un conjunto (en nuestro caso de elementos que utilizaremos para componer un mensaje) y $\otimes$ es una operación. En un grupo, independientemente de los elementos que consideremos, se cumple que:

- el resultado de aplicar $\otimes$ siempre pertenece al conjunto G,
- la operación $\otimes$ es asociativa,
- existe un elemento neutro de $\otimes$ para cualquier elemento,
- para todo elemento del conjunto existe un inverso de él respecto la operación.

Ejemplo 1. *Un ejemplos de grupo es $\langle \mathbb{Z}, + \rangle$. En efecto, la suma de cualquier par de enteros es un entero, la suma de enteros es asociativa, el 0 es el elemento neutro, y para todo $n \in \mathbb{Z}$, su inverso es $-n$ ya que $n + (-n) = 0$.*

Si consideramos un conjunto cualquiera y la operación permutación obtenemos también una estructura de grupo. Un ejemplo práctico de este grupo es el cubo de Rubik.

Ejemplo 2. *El par $\langle [1, 6], \cdot \text{ mód } 7 \rangle$ sí tiene estructura de grupo ya que el producto de cualquier par de números módulo 7 está en el intervalo $[1, 6]$, la operación es asociativa, el 1 es el elemento neutro, y para todo $n \in \mathbb{Z}$, existe su inverso:*

$$1 \cdot 1 \text{ mód } 7 = 1 \qquad 2 \cdot 4 \text{ mód } 7 = 1$$
$$3 \cdot 5 \text{ mód } 7 = 1 \qquad 4 \cdot 2 \text{ mód } 7 = 1$$
$$5 \cdot 3 \text{ mód } 7 = 1 \qquad 6 \cdot 6 \text{ mód } 7 = 1$$

Puede comprobarse que el par $\langle [1,9], \cdot \text{ mód } 10 \rangle$ *no tiene estructura de grupo. Su prueba es análoga a la anterior y se propone como ejercicio.*

En particular, en criptografía es de especial interés el conjunto $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ para un valor de n concreto y cualquiera. Considerando este conjunto como el de elementos que podemos utilizar para construir mensajes, una función sobre un elemento del conjunto puede dar como resultado un valor fuera del conjunto $\mathbb{Z}_n$, por lo que consideramos la *congruencia módulo* n como:

$$a \equiv b \pmod{n} \iff a - b = kn,\ k \in \mathbb{Z}$$

A partir de esta, puede definirse la *reducción módulo* n de un valor a, que denotaremos como:

$$a \text{ mód } n,$$

como el resto entero de dividir a por n.

También puede demostrarse fácilmente que la congruencia módulo n es una relación de equivalencia, esto es, cumple las propiedades reflexiva ($a \equiv a$ para cualquier elemento a), simétrica (si $a \equiv b$ entonces $b \equiv a$ para cualquier par de elementos a y b) y transitiva (si $a \equiv a$ y $b \equiv c$ entonces $a \equiv c$ para cualquier elección de a, b y c).

Considerando la congruencia módulo n, la suma y el producto son compatibles con la congruencia, esto es, dados a y b cualesquiera y sus reducciones $a \equiv a' \pmod{n}$ y $b \equiv b' \pmod{n}$, se cumple que:

- $a + b \equiv a' + b' \pmod{n}$
- $ab \equiv a'b' \pmod{n}$

o en otras palabras, la suma y el producto están bien definidos en $\mathbb{Z}_n$, por lo que podemos decir que en $\mathbb{Z}_n$:

- $[a]_{\equiv_n} + [b]_{\equiv_n} = [a + b]_{\equiv_n}$
- $[a]_{\equiv_n}[b]_{\equiv_n} = [ab]_{\equiv_n}$

A efectos prácticos, a partir de que la definición de la congruencia módulo n, del hecho que esta sea una relación de equivalencia y de que las operaciones suma y producto son compatibles con la congruencia, en cualquier operación módulo n podemos reducir los operandos módulo n en cualquier momento.

Ejemplo 3. *En el cálculo de* $(345331 + 2000100122) \cdot 12233312 \text{ mód } 45$*, podemos operar considerando los operandos indicados y luego reducir el resultado módulo* 45*, o bien podemos reducirlos todos previamente de acuerdo con el valor modular, aplicando al final, si es necesario otra reducción módulo* 45*. Esto es:*

$$\begin{aligned}&(345331 + 2000100122) \cdot 12233312 \text{ mód } 45 = \\ &(345331 \text{ mód } 45 + 2000100122 \text{ mód } 45) \cdot 1223311233312 \text{ mód } 45 = \\ &(1 + 17) \cdot 27 = 486 \text{ mód } 45 = 36.\end{aligned}$$

El hecho que la suma y el producto sean consistentes en $\mathbb{Z}_n$ no implica que tengan determinada estructura. De hecho, si bien $\langle \mathbb{Z}_n, + \rangle$ tiene estructura de grupo, $\langle \mathbb{Z}_n, \cdot \rangle$ no la tiene (como se muestra en el Ejemplo 2).

En conjunto, $(\mathbb{Z}_n, +, \cdot)$ posee estructura de anillo conmutativo, de esta forma puede resumirse que cumple las siguientes propiedades:

- La suma y el producto son operaciones cerradas y conmutativas en $\mathbb{Z}_n$.
- $(\mathbb{Z}_n, +)$ es un grupo (la operación es asociativa, tiene elemento neutro e inverso para todo valor en $\mathbb{Z}_n$).
- $(\mathbb{Z}_n, \cdot)$ es un semigrupo (la operación es asociativa y tiene elemento neutro).
- El producto distribuye respecto la suma.

Será interesante considerar aquellos valores de n para los que existe el inverso de todo (o casi todo) valor de $\mathbb{Z}_n$. En este sentido tendrá especial interés el siguiente teorema:

Teorema 1 (de congruencia lineal)**.** *La congruencia* $ax \equiv b \text{ (mód } n)$ *tiene una única solución si y sólo si* $mcd(a, n)$ *divide* b*.*

A partir de este resultado puede demostrarse que a tiene inverso para el producto módulo n si y sólo si a y n son *relativamente primos*, esto es si $mcd(a, n) = 1$.