AMPLIACIÓN DE MATEMÁTICAS

APLICACIÓN: OPERACIONES RÁPIDAS.

Consideramos $(\mathbb{Z}_n, +, \times)$ y la descomposición en producto de potencias de primos

$$n = p_1^{r_1} p_2^{r_2} .....p_k^{r_k}.$$

Con ello vamos a definir otro conjunto con nuevas operaciones.

Definición 1. *Se define el producto cartesiano*

$$\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times .... \times \mathbb{Z}_{p_k^{r_k}} = \prod_{j=1}^{k} \mathbb{Z}_{p_j^{r_j}}.$$

Sobre él definimos

una suma:

$$\begin{array}{rcccccc} + & : & \prod_{j=1}^k \mathbb{Z}_{p_j^{r_j}} \times \prod_{j=1}^k \mathbb{Z}_{p_j^{r_j}} & \to & \prod_{j=1}^k \mathbb{Z}_{p_j^{r_j}} & & \\ & & (([x_j]_{p_j^{r_j}})_{j=1}^k, ([y_j]_{p_j^{r_j}})_{j=1}^k) & \to & ([x_j]_{p_j^{r_j}})_{j=1}^k + ([y_j]_{p_j^{r_j}})_{j=1}^k & = & ([x_j + y_j]_{p_j^{r_j}})_{j=1}^k. \end{array}$$

un producto:

$$\begin{array}{rcccccc} \times & : & \prod_{j=1}^k \mathbb{Z}_{p_j^{r_j}} \times \prod_{j=1}^k \mathbb{Z}_{p_j^{r_j}} & \to & \prod_{j=1}^k \mathbb{Z}_{p_j^{r_j}} & & \\ & & (([x_j]_{p_j^{r_j}})_{j=1}^k, ([y_j]_{p_j^{r_j}})_{j=1}^k) & \to & ([x_j]_{p_j^{r_j}})_{j=1}^k \times ([y_j]_{p_j^{r_j}})_{j=1}^k & = & ([x_j y_j]_{p_j^{r_j}})_{j=1}^k. \end{array}$$

Vamos a ver que $(\mathbb{Z}_n, +, \times)$ se comporta algebraicamente igual que $(\prod_{j=1}^k \mathbb{Z}_{p_j^{r_j}}, +, \times)$, lo cuál se deduce del **Teorema Chino del Resto**. Esta forma de "descomponer " un conjunto la vamos a usar en más de una ocasión. Para hacer cálculo rápido, como veremos en este capítulo y el siguiente. Para la clasificación de grupos abelianos finitos que veremos en el siguiente tema. Y de allí a la caracterización de cuerpos finitos.

Teorema 1. *La aplicación*

$$\begin{array}{rcccc} T & : & \mathbb{Z}_n & \to & \prod_{j=1}^k \mathbb{Z}_{p_j^{r_j}} \\ & & [x]_n & \to & T([x]_n) = ([x]_{p_1^{r_1}}, [x]_{p_2^{r_2}}, ..., [x]_{p_k^{r_k}}) \end{array}$$

es un ***biyección*** *y verifica que para todo* $x = [x]_n, y = [y]_n \in \mathbb{Z}_n$

- $T(x+y) = T(x) + T(y)$
- $T(xy) = T(x)T(y)$.

Demostración: La aplicación está **bien definida** ya que si $[x]_n = [y]_n$ esto implica que $n|x-y$ y como $p_j^{r_j}|n$ para todo $j = 1, 2, ..., k$, se tiene que $[x]_{p_j^{r_j}} = [y]_{p_j^{r_j}}$ para todo j.

T es **inyectiva**, ya que si

$$([x]_{p_1^{r_1}}, [x]_{p_2^{r_2}}, ..., [x]_{p_k^{r_k}}) = ([y]_{p_1^{r_1}}, [y]_{p_2^{r_2}}, ..., [y]_{p_k^{r_k}})$$

esto quiere decir que x e y son ambas soluciones del mismo sistema de congruencias

$$x \equiv a_j \text{ mód. } p_j^{r_j}, \quad \text{para todo } \ j = 1, 2, .., k.$$

Como los $p_j^{r_j}$ son primos entre si el Teorema Chino del Resto nos dice que

$$x \equiv y \qquad \text{mód} \qquad p_1^{r_1} p_2^{r_2} .....p_k^{r_k} = n.$$

Es decir $[x]_n = [y]_n$.

T es **suprayectiva**, ya que para todo $(a_1, a_2, ..., a_k) \in \prod_{j=1}^{k} \mathbb{Z}_{p_j^{r_j}}$, el Teorema Chino del Resto nos dice que existe solución del sistema de congruencias

$$x \equiv a_j \text{ mód. } p_j^{r_j}, \quad \text{para todo } \ j = 1, 2, .., k.$$

y por tanto $T([x]_n) = (a_1, a_2, ..., a_k)$

Las propiedades $T(x+y) = T(x) + T(y)$ y $T(xy) = T(x)T(y)$ se tienen inmediatamente por al definición de la suma y el producto tanto en $(\mathbb{Z}_n, +, \times)$ como en $(\prod_{j=1}^{k} \mathbb{Z}_{p_j^{r_j}}, +, \times)\square$

Observación 1.

- Más adelante diremos que T es un **isomorfismo de anillos**. Lo que quiere decir que los conjunto que enlaza la aplicación T se comportan de la misma manera algebraicamente.
- Como T es **biyectiva**, también se verifica que $T^{-1}(T(x)+T(y)) = x+y$ y que $T^{-1}(T(x)T(y)) = xy$
- Lo anterior se puede aplicar a que toda operación sobre $\mathbb{Z}_n$ se puede transladar a $\prod_{j=1}^{k} \mathbb{Z}_{p_j^{r_j}}$ usando T y el resultado que se consigue llevarlo a $\mathbb{Z}_n$ por T^{-1}, siendo este último el resultado de la operación primitiva.

Veamos varios ejemplos para aclarar lo que estamos diciendo.

Ejercicio 1. *Tenemos que sumar* $[35]_{140} + [56]_{140}$.

Como los números son pequeños, $35+56 = 91$ y así $[35]_{140}+[56]_{140} = [91]_{140}$.

Otra forma de hacerlo es la siguiente. Como $140 = 4 \times 5 \times 7$

$$\begin{aligned}[35]_{140} + [56]_{140} &= T^{-1}\left(([35]_4, [35]_5, [35]_7) + ([56]_4, [56]_5, [56]_7)\right)\\ &= T^{-1}\left(([3]_4, [0]_5, [0]_7) + ([0]_4, [1]_5, [0]_7)\right)\\ &= T^{-1}\left(([3]_4, [1]_5, [0]_7)\right)\end{aligned}$$

y usando el Teorema Chino del Resto para resolver

$$x \equiv 3 \text{ mód } 4, \;\; x \equiv 1 \text{ mód } 5, \;\text{ y }\; x \equiv 0 \text{ mód } 7,$$

se tiene que

$$\begin{aligned}[35]_{140} + [56]_{140} &= [3 \times 35 \times 3 + 1 \times 28 \times 2]_{140}\\ = [315 + 56]_{140} &= [91]_{140} \qquad \begin{pmatrix} 371 & |\underline{140} \\ 91 & 2 \end{pmatrix} \square\end{aligned}$$

Ejercicio 2. *Tenemos que multiplicar* $[35]_{2052}[56]_{2052}$.

Como los números son pequeños, $35\times56 = 1960$ y así $[35]_{2052}[56]_{2052} = [1960]_{2052}$.

Otra forma de hacerlo es la siguiente. Como $2052 = 4 \times 27 \times 19$,

$$\begin{aligned}[35]_{2052} \times [56]_{2052} &= T^{-1}\left(([35]_4, [35]_{27}, [35]_{19})([56]_4, [56]_{27}, [56]_{19})\right)\\ &= T^{-1}\left(([3]_4, [8]_{27}, [16]_{19})([0]_4, [2]_{27}, [18]_{19})\right)\\ = T^{-1}\left(([0]_4, [16]_{27}, [3]_{19})\right) &\left(16 \times 18 = 288 \text{ y } \begin{matrix} 288 & |\underline{19} \\ 3 & 15 \end{matrix}\right)\end{aligned}$$

y usando el Teorema Chino del Resto para resolver

$$x \equiv 0 \text{ mód } 4, \;\; x \equiv 16 \text{ mód } 27, \;\text{ y }\; x \equiv 3 \text{ mód } 19,$$

se tiene que

$$\begin{aligned}[35]_{2052}[56]_{2052} &= [16 \times 76 \times [76]_{27}^{-1} + 3 \times 108 \times [108]_{19}^{-1}]_{2052}\\ &= [16 \times 76 \times [22]_{27}^{-1} + 3 \times 108 \times [13]_{19}^{-1}]_{2052}\end{aligned}$$

$$\begin{matrix} 27 & |\underline{22} \\ 5 & 1 \end{matrix} \qquad \begin{matrix} 22 & |\underline{5} \\ 2 & 4 \end{matrix} \qquad \begin{matrix} 5 & |\underline{2} \\ 1 & 2 \end{matrix}$$

i	0	1	2	3	4	
r_i	27	22	5	2	1	
q_i		1	4	2		
α_i	1	0	1	-4	9	
β_i	0	1	-1	5	-11	

$$\begin{array}{cc} 19 & |\underline{13} \\ 6 & 1 \end{array} \qquad \begin{array}{cc} 13 & |\underline{6} \\ 1 & 2 \end{array}$$

i	0	1	2	3	4	
r_i	19	13	6	1		
q_i		1	2			
α_i	1	0	1	-2		
β_i	0	1	-1	3		

y así tenemos que

$$= [16 \times 76 \times [-11]_{27} + 3 \times 108 \times 3]_{2052} = [16 \times 76 \times 16 + 972]_{2052}$$

$$= [19456 + 972] = [1960]_{2052} \qquad \begin{pmatrix} 20428 & |\underline{2052} \\ 1960 & 9 \end{pmatrix} \square$$

Observación 2. *Lo anterior, obviamente, no está pensado para multiplicar un par de números "chicos". La descomposición de* $\mathbb{Z}_n$ *en* $\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times .... \times \mathbb{Z}_{p_k^{r_k}}$ *está en la base de la* ***Computación en Paralelo****.*

Al final del próximo capítulo, con ayuda de la **función de Euler**, veremos como esta técnica nos permite hacer otros cálculos de forma rápida.

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

E-mail address: Cesar_Ruiz@mat.ucm.es