AMPLIACIÓN DE MATEMÁTICAS

GRUPO MULTIPLICATIVO. ELEMENTO Y POLINOMIO PRIMITIVO.

El grupo multiplicativo de un cuerpo finito tiene propiedades especiales.

Teorema 1. *Sea $\mathbb{F}$ un cuerpo finito de q elementos.*

- **a:** *El grupo multiplicativo $(\mathbb{F}^*, \times)$ de los elementos no nulos de $\mathbb{F}$ es un grupo cíclico de orden $q-1$.*
- **b:** *Todos los elementos de $\mathbb{F}$ son las q raíces del polinomio $x^q - x$.*

Demostración: Vamos a usar el Teorema de Clasificación de los Grupos Abelianos (ver Tema de Grupos).

$(\mathbb{F}^*, \times)$ es un grupo abeliano de orden $q-1$. Entonces se puede representar como

$$\mathbb{F}^* \backsimeq \mathbb{Z}_{d_1} \times .... \times \mathbb{Z}_{d_s}$$

de modo que $d_1 > 1$ y $d_i | d_{i+1}$ para $1 \leq i < s$ (también se tiene que $d_1 \times ... \times d_s = q-1$).

Ahora un elemento $a \in \mathbb{Z}_{d_1} \times .... \times \mathbb{Z}_{d_s}$ puede tener orden r que divide a d_1 o d_2 o....d_s, en cualquier caso $r | d_s$. Entonces para todo $a \in \mathbb{F}^*$,

$$a^{d_s} - 1 = 0.$$

El polinomio $x^{d_s} - 1$ sobre $\mathbb{F}$ puede tener a lo más d_s raíces, por tanto

$$|\mathbb{F}^*| = q - 1 \leq d_s.$$

Puesto que $d_s || \mathbb{F}^*|$, se tiene que $d_s \leq |\mathbb{F}^*|$. Por tanto deducimos que

$$|\mathbb{F}^*| = q - 1 = d_s,$$

y así

$$\mathbb{F}^* \backsimeq \mathbb{Z}_{d_s}.$$

Lo que prueba que $\mathbb{F}^*$ es cíclico. Es decir que existe en $\mathbb{F}^*$ un elemento de orden $q-1$, y en todo caso todo elemento de $\mathbb{F}^*$ elevado a $q-1$ da la unidad. Así como

$$x^q - x = x(x^{q-1} - 1),$$

se tiene que todos los elementos de $\mathbb{F}$ son las raíces del polinomio anterior $\square$

Ejemplo 1. *Sea* $\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2+x+1)$. *Hay que calcular* $[x]^{432}$.

El polinomio x^2+x+1 no tiene raíces en $\mathbb{Z}_2$, así es irreducible y tenemos que $\mathbb{Z}_2[x]/(x^2+x+1)$ es un cuerpo de cuatro elementos. $\mathbb{F}_4^*$ tiene tres elementos, uno de ellos es $[x]$. Podemos escribir

$$[x]^{432} = [x]^{144\times 3} = ([x]^3)^{144} = 1^{144} = 1 \ \square$$

Si consideramos los cuerpos finitos $\mathbb{Z}_p$, p primo, y sus grupos multiplicativos $(\mathbb{Z}_p^*, \times)$, entonces sabemos que existen elementos $a \in \mathbb{Z}_p^*$ de modo que

$$\mathbb{Z}_p^* = \{a, a^2, ..., a^{p-1} = 1\}.$$

Si hacemos la tabla

p	2	3	5	7	11	13	17
núm. "a"	1	1	2	2	..	..	..

hagamos el caso (como ejemplo) de $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$.

$$\begin{gathered} 1^1 = 1 \\ 2^3 = 1 \\ 3^6 = 1 \\ 4^3 = 1 \\ 5^6 = 1 \\ 6^2 = 1, \end{gathered}$$

así $a=3$ y $a=5$ son los únicos generadores de $\mathbb{Z}_7^*$.

La propiedad de generar todo el grupo multiplicativo cíclico de un cuerpo finito merece una definición.

Definición 1. *Sea* $\mathbb{F}$ *un cuerpo finito de característica* p.

- **a:** *A todo elemento de* $\mathbb{F}$ *generador del grupo multiplicativo se le llama* ***elemento primitivo*** *del cuerpo.*
- **b:** *Al polinomio mínimo de un elemento primitivo de* $\mathbb{F}$ *sobre* $\mathbb{Z}_p[x]$ *se le llama* ***polinomio primitivo****.*

Observación 1.

Como hemos visto en la tabla de arriba, un cuerpo no tiene muchos elementos primitivos. Al estudiar el Teorema de Lagrange relativo a Grupos, observamos que la cantidad de generadores de un grupo cíclico finito, en este caso del grupo multiplicativo de un cuerpo finito $(\mathbb{F}^*, \times)$, es precisamente $\phi(|\,\mathbb{F}^*|) = \phi(|\,\mathbb{F}| - 1)$, donde ϕ es la función de Euler. Tampoco es fácil hallarlos. Ni ellos ni sus correspondientes polinomios mínimos (¡claro para valores altos del cardinal de $\mathbb{F}$!). Por su rareza son útiles en **Criptografía.**

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
E-mail address: Cesar_Ruiz@mat.ucm.es