7.7.6. *Demostrar que los tres conjuntos descritos en los ejemplos 1,2,3 son de Sidon.*

Sea p un primo impar y g una raíz primitiva de $\mathbb{F}_p$.

Ejemplo 1: El conjunto de Sidon más sencillo que se conoce es el conjunto de p elementos

$$A = \{(x, x^2),\ x \in \mathbb{Z}_p\} \subset \mathbb{Z}_p \times \mathbb{Z}_p$$

Para ver que es un conjunto de Sidon, basta comprobar que si $(a_1, a_2) \neq (0, 0)$, entonces x_1 y x_2 quedan determinados en la ecuación $(x_1, x_1^2) - (x_2, x_2^2) = (a_1, a_2)$

Si $a_1 = 0$ y $a_2 \neq 0$, entonces la ecuación no tiene solución. Por tanto, $a_1 \neq 0 \implies a_1$ tiene inverso multiplicativo. Consecuentemente:

$$\left.\begin{array}{c} x_1 - x_2 = a_1 \\ x_1^2 - x_2^2 = a_2 \end{array}\right\} \implies \left.\begin{array}{c} x_1 - x_2 = a_1 \\ (x_1 + x_2)(x_1 - x_2) = a_2 \end{array}\right\} \implies$$

$$\implies \left.\begin{array}{c} x_1 - x_2 = a_1 \\ x_1 + x_2 = a_2 a_1^{-1} \end{array}\right\} \implies \left.\begin{array}{l} x_1 = \frac{1}{2} \cdot (a_1 + a_2 a_1^{-1}) \\ x_2 = \frac{1}{2} \cdot (a_2 a_1^{-1} - a_1) \end{array}\right\}$$

Ejemplo 2: A Golomb se debe el conjunto de Sidon de p-2 elementos

$$A = \{(x, y),\ g^x + q^y = 1\} \subset \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$$

Al igual que en el ejemplo 1, para ver que el conjunto es de Sidon es suficiente comprobar que, salvo cuando $(a_1, a_2) = (0, 0)$, la ecuación $(x_1, y_1) - (x_2, y_2) = (a_1, a_2)$ tiene a lo sumo una solución siempre y cuando $g^{x_1} + g^{y_1} = 1$ y $g^{x_2} + g^{y_2} = 1$

$$\left.\begin{array}{rcl} & & g^{x_1} + g^{y_1} = 1 \\ x_1 - x_2 = a_1 & \implies & \boxed{x_1 = a_1 + x_2} \\ y_1 - y_2 = a_2 & \implies & \boxed{y_1 = a_2 + y_2} \\ g^{x_2} + g^{y_2} = 1 & \implies & \boxed{g^{x_2} = 1 - g^{y_2}} \end{array}\right\}$$

Resolvemos el sistema:

$$g^{x_1} + g^{y_1} = 1 \implies g^{a_1 + x_2} + g^{a_2 + y_2} = 1 \implies$$

$$\implies g^{a_1} \cdot (1 - g^{y_2}) + g^{a_2} \cdot g^{y_2} = 1 \implies g^{a_1} - g^{y_2} g^{a_1} + g^{y_2} g^{a_2} = 1 \implies$$

$$\implies g^{y_2} \cdot (g^{a_2} - g^{a_1}) = 1 - g^{a_1}$$

Y de aquí deducimos que y_2 queda determinado siempre y cuando $a_1 \neq 0$ y $a_1 \neq a_2$ (de no verificarse estas condiciones, la ecuación no tendría solución, luego ya habríamos demostrado que el conjunto es de Sidon). Además, si y_2 tiene solución única, esta determina también de forma única x_1, x_2 y y_1.

Ejemplo 3: Welch descubrió el conjunto de Sidon de p-1 elementos

$$A = \{(x, g^x),\ 0 \leq x \leq p-1\} \subset \mathbb{Z}_{p-1} \times \mathbb{Z}_p$$

Sea $(a_1, a_2) \neq (0, 0)$, la ecuación $(x_1, g^{x_1}) - (x_2, g^{x_2}) = (a_1, a_2)$, determina x_1 y x_2 de forma única. Esto es, tenemos que ver que el siguiente sistema tiene, a lo sumo, una solución.

$$\left.\begin{array}{c} x_1 - x_2 \equiv a_1\ (mod\ p-1) \overset{Fermat}{\Longrightarrow} \quad g^{x_1-x_2} \equiv g^{a_1}\ (mod\ p) \\ g^{x_1} - g^{x_2} \equiv a_2\ (mod\ p) \end{array}\right\} \Longrightarrow$$

$$\Longrightarrow \left.\begin{array}{c} g^{x_1} \equiv g^{a_1+x_2}\ (mod\ p) \\ g^{x_1} - g^{x_2} \equiv a_2\ (mod\ p) \end{array}\right\} \Longrightarrow g^{a_1+x_2} - g^{x_2} \equiv a_2\ (mod\ p) \equiv$$

$$\equiv g^{x_2} \cdot (g^{a_1} - 1) = a_2\ (mod\ p)$$

Y, por el mismo razonamiento que en el ejemplo 2, el valor de x_2 queda determinado de forma única, y con él, también el valor de x_1.

Problema escrito por Jesús de los Nietos Valle.