AMPLIACIÓN DE MATEMÁTICAS

CUERPOS FINITOS. APLICACIONES.

En los modelos de la Física a la Ingeniería necesitamos usar $\mathbb{R}$ como conjunto de números ($\mathbb{R}$ es un cuerpo). Por la naturaleza de los números reales (números con parte entera y parte decimal finita o no) solo podemos aspirar a representarlos aproximadamente (coma flotante). En otros problemas, en cambio, los códigos que usamos son finitos y podemos emplear cuerpos finitos ($\mathbb{Z}_p$, p primo, por ejemplo) cuya representación en el ordenador es exacta, no aproximada.

Observación 1. *El* ***Álgebra Lineal*** *sobre cuerpos finitos es la misma que sobre* $\mathbb{R}$ *o* $\mathbb{C}$.

Proposición 1. *Sea* $\mathbb{F}$ *un cuerpo finito y sea*

$$f : \mathbb{F} \to \mathbb{F}$$

una aplicación. Entonces existe un ***polinomio*** $P \in \mathbb{F}[x]$ *de modo que*

$$f(x) = P(x) \qquad \textit{para todo} \qquad x \in \mathbb{F}.$$

Demostración: Como $\mathbb{F}$ es un cuerpo finito

$$\mathbb{F} = \{x_0, x_1, ...x_n\};$$

$\mathbb{F}$ tiene una cantidad finita de elementos distintos, pogamos que son $n+1$ (e.d. card$\mathbb{F} = n+1$).

Sea $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ un polinomio con coeficientes en $\mathbb{F}$ ($P \in \mathbb{F}[x]$, lo que quiere decir que $a_0, a_1.., a_n \in \mathbb{F}$). Si forzamos que

$$P(x_i) = f(x_i) = y_i \in \mathbb{F} \qquad \text{para todo} \qquad i = 0, 1, 2, ..., n$$

entonces tendremos un sistema lineal de $n+1$ ecuaciones con $n+1$ incógnitas: $a_0, a_1, .., a_n$.

$$\begin{array}{ccccccccc} a_0 & + & a_1 x_0 & + & \cdots & + & a_n x_0^n & = & y_0 \\ a_0 & + & a_1 x_1 & + & \cdots & + & a_n x_1^n & = & y_1 \\ \vdots & & & & \cdots & & & & \\ a_0 & + & a_1 x_n & + & \cdots & + & a_n x_n^n & = & y_n \end{array}$$

o equivalentemente en forma matricial

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ \vdots & & & \cdots & \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Este sistema lineal tiene por por matriz de coeficientes una matriz de Vandermonde, la cuál tiene determinante no nulo ya que $x_i \neq x_j$ si $i \neq j$. Por lo tanto el sistema tiene solución única (Teorema de Rouche), la cuál determina de forma unívoca al polinomio $P\square$

Observación 2. *Todas las funciones que uno pueda imaginar sobre un cuerpo finito $\mathbb{F}$ se reducen a sumas y productos. Lo cuál es "sencillo" de computar.*

Referencias

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

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