AMPLIACIÓN DE MATEMÁTICAS

POLINOMIOS SOBRE CUERPOS FINITOS. APLICACIONES.

Ya vimos que cualquier función sobre un cuerpo finito es una aplicación polinómica. Vamos a insistir sobre este hecho.

Teorema 1. *Si $\mathbb{F}$ es un cuerpo finito y*

$$(a_0, b_0), (a_1, b_1), ..., (a_k, b_k) \in \mathbb{F} \times \mathbb{F}$$

de modo que $a_i \neq a_j$, cuando $i \neq j$, entonces existe un único polinomio $p \in \mathbb{F}[x]$, con grado menor o igual a k, de modo que

$$\overline{p}(a_i) = b_i \qquad \textit{para todo} \qquad i = 0, 1, 2, ..., k.$$

Demostración:

Álgebra Lineal: Sea $P(x) = c_0 + c_1 x + ... + c_k x^k \in \mathbb{F}[x]$, de modo que

$$\overline{P}(a_i) = b_i = c_0 + c_1 a_i + ... + c_k a_i^k \qquad \text{para todo} \qquad i = 0, 1, 2, ..., k.$$

Tenemos por tanto un sistema lineal de $k+1$ ecuaciones con $c_0, c_1, ..., c_k$ incógnitas,

$$\begin{pmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^k \\ 1 & a_1 & a_1^2 & \cdots & a_1^k \\ \vdots & & & & \\ 1 & a_k & a_k^2 & \cdots & a_k^k \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_k \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_k \end{pmatrix}$$

que tiene una solución única. Claro, el determinante de los coeficientes es un determinante de Vandermonde que no es nulo si $a_i \neq a_j$ para todo $i \neq j$ (Ver Álgebra Lineal de un primer curso).

Fórmula de interpolación de Lagrange: Otra forma de calcular P, con menos conste de operaciones es la que sigue. Para cada $i = 0, 1, 2, ..., k$ se define el polinomio

$$P_i(x) = \frac{(x - a_0)(x - a_1)....(x - a_{i-1})(x - a_{i+1}).....(x - a_k)}{(a_i - a_0)(a_i - a_1)....(a_i - a_{i-1})(a_i - a_{i+1}).....(a_i - a_k)}.$$

Estos polinomios verifican que $\overline{P_i}(a_i) = 1$ y $\overline{P_i}(a_j) = 0$ para todo $j \neq i$. Además $grad.P_1 = k$. El polinomio que buscamos P es

$$P(x) = b_0P_0(x) + b_1P_1(x) + ... + b_kP_k(x).$$

El polinomio P tiene grado menor o igual a k, y ahora es claro que

$$P(a_i) = b_iP_i(a_i) = b_i \qquad \text{para todo} \qquad i = 0, 1, 2, ..., k \ \square$$

Corolario 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*

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

(Observemos que P no tiene por que ser único).

Demostración: Si el cuerpo es finito, se tiene que

$$\mathbb{F} = \{a_0, a_1, ..., a_k\}.$$

Sea $b_i = f(a_i)$ para $i = 0, 1, 2, ..., k$. Sabemos que existe $P \in \mathbb{F}[x]$ (único de grado menor o igual a k; pero puede haber otros de grados superiores) de modo que $\overline{P}(a_i) = b_i$ para todo $i = 0, 1, ..., k \ \square$

Observación 1. *Se puede probar que un cuerpo $\mathbb{F}$ es finito si y solo si toda aplicación sobre él es una aplicación polinómica.*

El corolario de arriba nos da una parte de la prueba. La otra se basa en que si $Card.\mathbb{F} = \infty$, tomando un subconjunto $A \subsetneq \mathbb{F}$ infinito, entonces la función

$$f(x) = \begin{cases} 1 & \text{si} \quad x \in A \\ 0 & \text{si} \quad x \notin A \end{cases}$$

esta bien definida, pero no puede ser una ecuación polinómica ya que las ecuaciones polinómicas tiene un número finito de raíces $\square$.

APLICACIÓN: SEGURIDAD CON ALGORITMOS.

Esta aplicación se podría llamar "**como dividir un secreto**".

Consideremos un lugar central de una organización o empresa (la "caja fuerte", por ejemplo). Supongamos que este lugar solo se puede alcanzar si al menos k empleados de un total de n están presentes al mismo tiempo. Una forma de acceso puede ser la siguiente.

Tomamos un primo p grande. Así tenemos que $\mathbb{Z}_p$ es un cuerpo finito. Las aplicaciones de $\mathbb{Z}_p$ en si mismo son todas polinómicas y hay en total p^p de ellas (p^p, puede ser un número muy grande).

Se toma $m \in \mathbb{Z}_p$ (la "**llave maestra**"). Se fabrica un polinomio de grado $k-1$

$$q(x) = m + c_1 x_1 + ... + c_{k-1} x^{k-1} \in \mathbb{Z}_p[x].$$

A los n empleados que van a tener acceso a la caja fuerte se les dá a cada uno una "subllave"

$$s_i = \overline{q}(i) \qquad i = 1, 2, 3, ..., n.$$

Observamos que si p es mucho más grande que n, entonces los $1, 2, .., n \in \mathbb{Z}_p$ son todos distintos.

Ahora si al menos k empleados están presentes, pueden juntar sus k subllaves de modo que pueden reconstruir el polinomio q y por tanto encontar la "llave maestra" $m = \overline{q}(0)$. Claro, sean $n_1, n_2, ..., n_k$ empleados. Juntos conocen

$$s_{n_i} = \overline{q}(n_i) \qquad i = 1, 2, ..., k \qquad \text{subllaves}$$

y existe un único polinomio q de grado a lo más $k-1$ de modo que coincida con las subllaves. Es nuestro polinomio q de partida. Este ejemplo está dado por Shamir en 1979.

Observación 2. *Periódicamente se pueden generar (o cambiar) nuevos p, m y q de forma aleatoria y asignar nueva subllaves $s_1, .., s_n$. Lo que incrementa la seguridad del proceso.*

Referencias

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

Email address: Cesar_Ruiz@mat.ucm.es