AMPLIACIÓN DE MATEMÁTICAS

TEOREMA CHINO DEL RESTO PARA POLINOMIOS.

De forma análoga a lo que ocurre en $\mathbb{Z}$, tenemos un Teorema Chino del Resto para polinomios. La prueba del teorema es igual que la dada para números enteros. Además, los cálculos asociados se hacen de igual manera; usando el algoritmo de Euclides para polinomios.

Una aplicación de este Teorema Chino del Resto la podemos encontrar en el **algoritmo de Berlekamp** de factorización de polinomios con coeficientes en cuerpos finitos.

Teorema 1. *(**Chino del Resto para polinomios.**)Sean $f_1, f_2, .., f_k \in \mathbb{F}[x]\backslash\{0\}$, k polinomios sobre un cuerpo $\mathbb{F}$ de modo que*

$$m.c.d(f_i, f_j) = 1 \qquad para\ todo \qquad i \neq j,$$

es decir "primos" entre si. Sean $g_1, g_2, ..., g_k \in \mathbb{F}[x]$ y se plantean las siguientes k ecuaciones en congruencias

$$h \equiv g_i\ m\acute{o}d.\ f_i\ (\Leftrightarrow f_i | h - g_i), \quad para\ todo\ \ i = 1, 2, .., k.$$

Entonces este sistema tiene solución. Además si h_1 y h_2 son dos soluciones de las ecuaciones anteriores se tiene que

$$h_1 \equiv h_2 \qquad m\acute{o}d. \qquad m.c.m(f_1, f_2, ..., f_k) = f_1 f_2 ....f_k.$$

Observación 1. *La **demostración, que sigue**, de este Teorema nos dice como resolver las ecuaciones en congruencias del enunciado. Es una demostración constructiva. Es la misma que para números enteros.*

Demostración: Sea $f = f_1 f_2 ...f_k$ el producto de los k polinomios (que en este caso, al ser primos entre si, coincide con el $m.c.m.$ de todos ellos). Sea

$$q_i = \frac{f}{f_i} \qquad \text{para} \qquad i = 1, 2, ..., k.$$

Como $m.c.d.(q_i, f_i) = 1$, existe $r_i \in \mathbb{F}[x]$ con la propiedad de que

$$q_i r_i \equiv 1 \text{ mód. } f_i, \qquad i = 1, 2, ..., k.$$

Claro, el Lema de Bezout nos dice que existen $r_i, s_i \in \mathbb{F}[x]$ de modo que

$$m.c.d.(q_i, f_i) = 1 = r_i q_i + s_i f_i.$$

Definimos ahora el polinomio h por

$$h = \sum_{i=1}^{k} g_i q_i r_i = g_1 q_1 r_1 + g_2 q_2 r_2 + ... + g_k q_k r_k.$$

Veamos que h es la solución (una de las soluciones) buscada. Como $f_i | q_j$ para $i \neq j$, se tiene que

$$h \equiv g_i q_i r_i \text{ mód. } f_i,$$

como $q_i r_i \equiv 1$ mód. f_i, se sigue que

$$h \equiv g_i \text{ mód. } f_i, \qquad \text{para todo} \qquad i = 1, 2, ..., k.$$

Ahora si h_2 es otra solución de todas las ecuaciones en congruencias,

$$h_2 \equiv g_i \text{ mód. } f_i, \qquad \text{para todo} \qquad i = 1, 2, ..., k$$

entonces

$$f_i | h - h_2 \qquad \text{para todo} \qquad i = 1, 2, ..., k.$$

Lo cuál implica que $m.c.m(f_1, f_2, ..., f_k) = f | h - h_2$, es decir

$$h \equiv h_2 \qquad \text{mód.} \qquad f_1 f_2 .... f_k \square$$

Ejemplo 1. *Queremos encontrar en* $\mathbb{Z}_3[x]$ *un polinomio de grado menor o igual a* 5*, llamemosle* h*, de modo que*

$$\begin{array}{rcl} h & \equiv & x^2 + x + 1 \quad mód \qquad x^3 \\ h & \equiv & x^2 + x + 1 \quad mód \quad x^3 + 2x + 1 \end{array}$$

Sea $h(x) = x^2 + x + 1$. Este polinomio verifica evidentemente las dos ecuaciones en congruencias anteriores (el grado de h es menor que 3). Si ahora h_2 es otra solución, como $m.c.d.(x^3, x^3 + 2x + 1) = 1$ (ya que x^3 solo es divisible por potencias de la x y $\alpha = 0$ no es raíz de $x^3 + 2x + 1$), entonces por el teorema Chino del Resto se tiene que

$$h_2 \equiv h \qquad \text{mód.} \qquad x^3(x^3 + 2x + 1) = x^6 + 2x^4 + x^3,$$

lo que quiere decir que existe $q \in \mathbb{Z}_3[x]$ de modo que

$$h_2(x) = x^2 + x + 1 + q(x)(x^6 + 2x^4 + x^3).$$

Así, salvo que $q = 0$, $grad.h_2 \geq 6$. La solución que buscamos es por tanto $h(x) = x^2 + x + 1$ □

Referencias

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

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