AMPLIACIÓN DE MATEMÁTICAS

TEOREMA CHINO DEL RESTO.

El Teorema que sigue se empleó en China al menos desde el siglo III. Tiene importantes aplicaciones, como veremos: cálculo rápido, algoritmo R.S.A. ...etc

Teorema 1. *(**Chino de los Restos.**)Sean* $n_1, n_2, .., n_k \in \mathbb{N}\backslash\{0\}$, k *números naturales de modo que*

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

es decir primos entre si. Sean $a_1, a_2, ..., a_k \in \mathbb{Z}$ *y se plantean las siguientes* k *ecuaciones en congruencias*

$$x \equiv a_i\ m\acute{o}d.\ n_i, \quad para\ todo\ \ i = 1, 2, .., k.$$

Entonces este sistema tiene solución. Además si x *e* y *son dos soluciones de las ecuaciones anteriores se tiene que*

$$x \equiv y \qquad m\acute{o}d. \qquad m.c.m.(n_1, n_2, ..., n_k) = n_1 n_2 .... n_k.$$

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

Demostración: Sea $n = n_1 n_2 ... n_k$ el producto de los k números (que en este caso, al ser primos entre si, coincide con el m.c.m. de todos ellos). Sea

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

Como $m.c.d.(q_i, n_i) = 1$, existe r_i el inverso de q_i en $\mathbb{Z}_{n_i}$, es decir

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

Definimos ahora el número entero x por

$$x = \sum_{i=1}^{k} a_i q_i r_i = a_1 q_1 r_1 + a_2 q_2 r_2 + ... + a_k q_k r_k.$$

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

$$x \equiv a_i q_i r_i \text{ mód. } n_i,$$

como $q_i r_i \equiv 1 \text{ mód. } n_i$, se sigue que

$$x \equiv a_i \text{ mód. } n_i, \qquad \text{para todo} \qquad i = 1, 2, ..., k.$$

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

$$y \equiv a_i \text{ mód. } n_i, \qquad \text{para todo} \qquad i = 1, 2, ..., k$$

entonces

$$n_i|x - y \qquad \text{para todo} \qquad i = 1, 2, ..., k.$$

Lo cuál implica que $m.c.m.(n_1, n_2, ..., n_k)|x - y$, es decir

$$x \equiv y \qquad \text{mód.} \qquad n_1 n_2 ....n_k \square$$

Ejercicio 1. *Nos piden encontrar x de modo que*

$$\begin{array}{rcl} x & \equiv & 2 \quad mód \quad 5 \\ 2x & \equiv & 1 \quad mód \quad 7 \\ 3x & \equiv & 4 \quad mód \quad 11 \end{array}$$

Como 5,7 y 11 son primos, podemos encontrar $[2]_7^{-1} = 4$ y $[3]_{11}^{-1} = 4$ de modo que el sistema de arriba queda

$$\begin{array}{rcl} x & \equiv & 2 \quad \text{mód} \quad 5 \\ x & \equiv & 4 \quad \text{mód} \quad 7 \\ x & \equiv & 4 \times 4 \equiv 5 \quad \text{mód} \quad 11. \end{array}$$

Ahora podemos aplicar el Teorema Chino del Resto. Así,

$$m.c.d.(5, 7 \times 11) = 1 \text{ y por tanto } 31 \times 5 - 2 \times 77 = 1,$$

$$m.c.d.(7, 5 \times 11) = 1 \text{ y por tanto } 8 \times 7 - 55 = 1$$

y

$$m.c.d.(11, 5 \times 7) = 1 \text{ y por tanto } 16 \times 11 - 5 \times 35 = 1.$$

Lo anterior se calcula a "ojo", o si no se "ve" se utiliza el algoritmo de Euclides. Tomando

$$x = 2(-2 \times 77) + 4(-55) + 5(-5 \times 35)$$

$$= 2(-154) + 4(-55) + 5(-175)$$

$$= -308 - 220 - 875 = -1403.$$

Y así el resultado buscado es $(5 \times 7 \times 11 = 385)$

$$x \equiv -1403 \text{ mód. } 385$$

y como

$$\begin{array}{rr} -1403 & |\underline{385} \\ 137 & -4 \end{array}$$

concluimos que

$$x \equiv 137 \text{ mód. } 385\square$$

Ejercicio 2. *Estando en U.S.A. el Sr. Herrera cambio un cheque de viaje. El cajero al pagarle confundio el número de dolares con los centavos y viceversa. El Sr. Herrera gasto 68 centavos en sellos y comprobó que el dinero que le quedaba era el doble del importe del cheque de viaje que había cambiado. ¿Qué valor mínimo tenía el cheque de viaje?*

Escribimos

$$C = a + \frac{b}{100}$$

donde C es el valor del cheque, a los dolares y b los centavos $(a, b \geq 0)$. Ahora lo que le dieron menos lo que gasto el Sr. Herrera en sellos es el doble de que le debieron dar, es decir

$$b + \frac{a}{100} - \frac{68}{100} = 2(a + \frac{b}{100})$$

operando llegamos a que

$$98b - 199a = 68 \qquad (*)$$

La ecuación anterior se conoce como **ecuación Diofántica lineal**. Este nombre lo que indica es que tenemos una ecuación lineal, cuya solución usual sería una recta en el plano, de la cuál solo nos interesan sus soluciones enteras, es decir soluciones $a, b \in \mathbb{N}$. Fijandonos, vemos que $(*)$ es lo mismo que decir que

$$98b \equiv 68 \quad \text{mód} \quad 199.$$

Ahora, tenemos que $m.c.d.(98, 199) = 1$, ya que usando el algoritmo de Euclides

$$\begin{array}{rr} 199 & |\underline{98} \\ 3 & 2 \end{array} \qquad \begin{array}{rr} 98 & |\underline{3} \\ 2 & 32 \end{array} \qquad \begin{array}{rr} 3 & |\underline{2} \\ 1 & 1 \end{array}$$

y así tenemos que

i	0	1	2	3	4	
r_i	199	98	3	2	1	
q_i		2	32	1	1	
α_i	1	0	1	-32	33	
β_i	0	1	-2	65	-67	

y conseguimos que

$$33 \times 199 - 67 \times 98 = 1.$$

Esto nos dice que el inverso de 98 módulo 199 es el -67 o lo que lo mismo el 132. Así nuestra ecuación Diofántica se reduce a

$$b \equiv 132 \times 68 \equiv 21 \qquad \text{mód} \qquad 199 \qquad \left(\begin{array}{cc} 132 \times 68 = 8976 & |\underline{199} \\ 21 & 45 \end{array} \right).$$

El menor valor que puede tomar $b = 21$ ($b = k199 + 21$). Por otro lado, de $(*)$

$$a = \frac{1}{199}(98 \times (k199 + 21) - 68) = 98k + 10.$$

Para $k = 0$, se obtiene los valores más pequeños y positivos de a y b, es decir $a = 10$ y $b = 21$. Así el número buscado $C = 10, 21\$$

Referencias

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

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