TEOREMA CHINO DEL RESIDUO

Por: Arturo Martinez C.

Al leer gran parte de la ya popularmente conocida como Matemática moderna, con sus intrincados conceptos y su extraña simbolización, fácilmente se cae en la tentación de suponerla 'inventada' por alguno de los muy brillantes genios de los últimos siglos, digamos del XVIII en adelante. Esta nota pretende presentar un concepto que ya en el siglo I d.c. era conocido y manipulado por los matemáticos chinos, siendo tal la razón para su nombre. Para su demostración, por supuesto, se utilizará la notación "moderna".

Si m, a, b son enteros, con m positivo, se dice que "a es congruente con b, módulo m", si m divide la diferencia $a-b$. Este concepto se denota por $a \equiv b \ (\text{mód } m)$ y no es difícil verificar que tal "congruencia módulo m" define una relación de equivalencia y por tanto induce una partición de $\mathbb{Z}$, cuyas clases de equivalencia se denotan por $[x]_m$, esto es:
$[x]_m = \{ y \in \mathbb{Z} / x \equiv y \ (\text{mód } m) \} = \{ y \in \mathbb{Z} / y = x + mk, \ k \in \mathbb{Z} \}$.

Asi, por ejemplo, para $m=5$ se tiene:

$[0]_5 = \{ y \in \mathbb{Z} / y = 0 + 5k, \ k \in \mathbb{Z} \} = \{ \dots, -10, -5, 0, 5, 10, \dots \}$

$[1]_5 = \{ y \in \mathbb{Z} / y = 1 + 5k, \ k \in \mathbb{Z} \} = \{ \dots, -9, -4, 1, 6, 11, \dots \}$

$[2]_5 = \{ y \in \mathbb{Z} / y = 2 + 5k, \ k \in \mathbb{Z} y = \{ \dots, -8, -3, 2, 7, 12, \dots \}$

$[3]_5 = \{ y \in \mathbb{Z} / y = 3 + 5k, \ k \in \mathbb{Z} \} = \{ \dots, -7, -2, 3, 8, 13, \dots \}$

$[4]_5 = \{ y \in \mathbb{Z} / y = 4 + 5k, \ k \in \mathbb{Z} \} = \{ \dots, -6, -1, 4, 9, 14, \dots \}$

Obsérvese que $[5]_5 = \{ y \in \mathbb{Z} / y = 5 + 5k, \ k \in \mathbb{Z} \} = \{ y \in \mathbb{Z} / y = 5(1+k), \ k \in \mathbb{Z} \} = \{ y \in \mathbb{Z} / y = 5k', \ k' \in \mathbb{Z} \} = [0]_5 = [10]_5 = [15]_5 = \cdots$. Análogamente, se tiene $[6]_5 = [11]_5 = [16]_5 = \cdots = [1]_5$; $[7]_5 = [12]_5 = [17]_5 = \cdots = [2]_5$, etc. ; y por tanto $\mathbb{Z}_5 = \{ [0]_5, [1]_5, [2]_5, [3]_5, [4]_5 \}$ es la partición de $\mathbb{Z}$ inducida por la relacion de equivalencia "congruencia módulo 5". Generalizando este ejemplo, se tiene que $\mathbb{Z}_m = \{ [0]_m, [1]_m, [2]_m, \dots, [m-1]_m \}$ es la partición de $\mathbb{Z}$ inducida por la relación de equivalencia "congruencia módulo m".

En lo que sigue se utilizarán estos conceptos:

I) m es un entero positivo.
II) $d = (a, b)$: d es el m.c.d. de a y b.
III) $d = (a, b) \Rightarrow (\exists x, y \in \mathbb{Z})(ax + by = d)$
IV) $(\forall a \in \mathbb{Z})(a \equiv a \ (\text{mód } m))$

PROPOSICION 1: Sean a, b, c, d, k enteros, entonces:

(i) $a \equiv b \ (\text{mód } m)$ implica que $ka \equiv kb \ (\text{mód } m)$
(ii) $a \equiv b \ (\text{mód } m)$ y $c \equiv d \ (\text{mód } m)$, implica que $(a+c) \equiv (b+d) \ (\text{mód } m)$ y $ac \equiv bd \ (\text{mód } m)$
(iii) $ac \equiv bc \ (\text{mód } m)$, con $(c, m) = 1$, implica que $a \equiv b \ (\text{mód } m)$.
(iv) $a \equiv b \ (\text{mod } km)$, con $k \neq 0$, implica que $a \equiv b \ (\text{mód } m)$.

Demostración (iii) :
Dado que $(c, m) = 1$, por III se tiene que $(\exists x, y \in \mathbb{Z})(cx + my = 1)$, luego $cx - 1 = my$ y por tanto $cx \equiv 1 \ (\text{mód } m)$. Utilizando (i) en éste resultado y en la hipótesis se obtienen las congruencias $acx \equiv a \ (\text{mód } m)$, $bcx \equiv b \ (\text{mod } m)$ y $acx \equiv bcx \ (\text{mód } m)$, a partir de las cuales la propiedad transitiva de la relación de equivalencia garantiza que $a \equiv b \ (\text{mód } m)$.

PROPOSICION 2: La congruencia $ax \equiv 1 \ (\text{mód } m)$ tiene solución si y solo sí $(a, m) = 1$.

Demostración:

$ax \equiv 1 \pmod m \iff (\exists y \in \mathbb{Z})(ax - 1 = my) \iff (\exists y \in \mathbb{Z})(ax + m(-y) = 1)$
$\iff (a, m) = 1.$

COROLARIO: Si p es primo, la congruencia $ax \equiv 1 \pmod p$ tiene solución para todo a no divisible por p.

El siguiente resultado presenta una versión más precisa y elegante de la propiedad establecida en el corolario. Se le conoce como el "Teorema de Fermat" en honor al gran matemático francés Pierre de Fermat (1601-1665), iniciador además de la teoría de los números y del cálculo de probabilidades. Uno de sus planteamientos, conocido como "el último problema de Fermat", establece que no existen tres números naturales, x, y, z, tales que $x^n + y^n = z^n$ para $n > 2$. Este problema subsiste sin demostración y sobre él la Sociedad Colombiana de Matemáticas prepara una monografía, de la cual ha sido encargado el Dr. Marco Fidel Suárez R., profesor de la Universidad del Valle, quien propuso a quienes integramos el grupo de álgebra durante el X coloquio de Matemáticas aunar esfuerzos en tal dirección.

TEOREMA DE FERMAT: Si p es primo y x no es divisible por p, entonces $x^{p-1} \equiv 1 \pmod p$.

Demostración:
Sean $[a_1]_p, [a_2]_p, \ldots, [a_{p-1}]_p$ las clases de equivalencia no-nulas de $\mathbb{Z}_p$ y sea $[x]_p$ una cualesquiera de ellas. Puesto que, para $1 \le i \le p-1$, $[x]_p [a_i]_p$ está en $\mathbb{Z}_p$, entonces

$$\prod_{i=1}^{p-1} [a_i]_p = \prod_{i=1}^{p-1} [x]_p [a_i]_p = [x]_p^{p-1} \prod_{i=1}^{p-1} [a_i]$$

y por tanto $[x]_p^{p-1} = [1]_p$, esto es, $x^{p-1} \equiv 1 \pmod p$.

COROLARIO: Si p es primo, entonces para todo x en $\mathbb{Z}$ se tiene que $x^p \equiv x \pmod p$.

Según el teorema de Fermat, si p es primo y $(a, p) = 1$, la congruencia $ax \equiv 1 \pmod p$ tiene como solución los valores $x \equiv a^{p-2} \pmod p$ y por tanto $ax \equiv b \pmod p$ tiene como solución los valores $x \equiv a^{p-2} b \pmod p$. Así, por ejemplo, las soluciones de $2x \equiv 4 \pmod 5$ son $x \equiv 2^3 \cdot 4 \pmod 5$, esto es, los enteros en $[2]_5$.

Utilizando ahora las proposiciones 1 y 2 se establece la siguiente propiedad:

PROPOSICION 3: Si $(a, m) = 1$, entonces para todo b la congruencia $ax \equiv b \pmod m$ tiene solución y tal solución es única módulo m.

Demostración:
Por la proposición 2 la congruencia $ax \equiv 1 \pmod m$ tiene solución, digamos x_0. Puesto que de $ax_0 \equiv 1 \pmod m$ se obtiene que $abx_0 \equiv b \pmod m$, los valores $x \equiv bx_0 \pmod m$ son soluciones de $ax \equiv b \pmod m$, y esto demuestra lo correspondiente a la existencia. Por otra parte, si $ax_1 \equiv b \pmod m$ y $ax_2 \equiv b \pmod m$ entonces (proposición 1 (ii)) $ax_1 - ax_2 \equiv (b - b) \pmod m$, esto es, $a(x_1 - x_2) \equiv 0 \pmod m$. Puesto que $(a, m) = 1$ la proposición 1 (iii) garantiza que $(x_1 - x_2) \equiv 0 \pmod m$ y por tanto $x_1 \equiv x_2 \pmod m$, lo cual demuestra la unicidad módulo m.

Finalmente, supóngase que se tienen varias congruencias en una misma variable pero respecto a diferentes módulos: $a_i x \equiv b_i \pmod{m_i}$, $i = 1, 2, \ldots, n$. Si para cada i se tiene que $(a_i, m_i) = 1$, la aplicación a cada congruencia del método establecido en la proposición 3 conduce a su respectiva solución. Por otra parte, si para $i \neq j$ se tiene que $(m_i, m_j) = 1$, puede determinarse una solución común para todas las n congruencias, a la cual se llega fácilmente mediante la generalización del siguiente resultado, tema central de esta nota:

TEOREMA CHINO DEL RESIDUO: Si $(m_1, m_2) = 1$, entonces las congruencias $x \equiv b \pmod{m_1}$ y $x \equiv c \pmod{m_2}$ tienen solución común, la cual es única módulo $m_1 m_2$.

Demostración:
Las soluciones generales de las dos congruencias son, respectivamente, $x = m_1 k + b$ y $x = m_2 q + c$, con $k, q \in \mathbb{Z}$. Igualando estos resultados para obtener la solución común, se obtiene que $m_1 k - (c-b) = m_2 q$, luego $m_1 k \equiv (c-b) \pmod{m_2}$. Dado que $(m_1, m_2) = 1$, la proposición 3 garantiza la existencia de un valor para k, único módulo m_2, que la satisface. Por otra parte, si x_1 y x_2 son soluciones comunes de las congruencias dadas, es decir, si $x_1 \equiv b \pmod{m_1}$, $x_1 \equiv c \pmod{m_2}$, $x_2 \equiv b \pmod{m_1}$ y $x_2 \equiv c \pmod{m_2}$, entonces m_1 y m_2 dividen tanto x_1 como a x_2, con $(m_1, m_2) = 1$, luego $m_1 m_2$ tambien divide a x_1 y a x_2; se tiene entonces que $m_1 m_2$ divide a la diferencia $x_1 - x_2$ y por tanto $x_1 \equiv x_2 \pmod{m_1 m_2}$, con lo cual se demuestra que la solución común de las dos congruencias es única módulo $m_1 m_2$.

Sorprendente o no, como ya se dijo, este resultado fue manejado con destreza por matemáticos de hace casi 20 siglos. ¿con cuántos otros conceptos "modernos" habrá ocurrido algo semejante? Y, mas intrigante aún, ¿mediante que medios, matemáticos o nó, fueron establecidos en tal época? Quizás un poco de ciencia-ficción a la moderna pueda darnos alguna respuesta que nos satisfaga...

C/ p.j.r.