Conferencia 5 - Sistemas Residuales

October 15, 2025

Definición. *Un **Sistema Residual Completo** módulo n, SRC(n), con* $n \in \mathbb{Z}_+$*, es un conjunto de* n *enteros incongruentes módulo* n

Teorema. *Sean* $n \in \mathbb{Z}_+$, $k \in \mathbb{Z}$, $(k, n) = 1$ *y* $\{a_1, a_2, \ldots, a_n\}$ *un sistema residual completo módulo* n*, entonces* $\{ka_1, ka_2, \ldots, ka_n\}$ *es también un sistema residual completo módulo* n*.*

Demostración
Supongamos que $\{ka_1, ka_2, \ldots, ka_n\}$ no es un SRC(n)
entonces existen i,j tales que $ka_i \equiv ka_j\,(n)$
como $(k, n) = 1$ entonces $a_i \equiv a_j\,(n)$
luego $\{a_1, a_2, \ldots, a_n\}$ tampoco es un SRC(n),
por tanto, por contrarecíproco, si $\{a_1, a_2, \ldots, a_n\}$ es un SRC(n)
entonces $\{ka_1, ka_2, \ldots, ka_n\}$ también lo es

Definición. *Una ecuación de la forma* $ax \equiv b\,(n)$ *con* $a, b \in \mathbb{Z}$ *y* $n \in \mathbb{Z}_+$ *es una ecuación lineal congruencial si se trata de resolver en enteros. Dos soluciones se consideran distintas si son incongruentes módulo* n*.*

Teorema. *La ecuación lineal congruencial* $ax \equiv b\,(n)$ *es soluble si y solo si* $(a, n)|b$

Demostración
$ax \equiv b\,(n)$ tiene solución si existe x_0 tal que $ax_0 \equiv b\,(n)$
entonces $n|ax_0 - b$ por lo que existe y_0 tal que $ax_0 - b = ny_0$
entonces como $ax_0 - ny_0 = b$
esta ecuación tiene solución si y solo si $(a, n)|b$

Note que si x_0 es solución de $ax \equiv b\,(n)$ y $x_1 \equiv x_0\,(\frac{n}{mcd(a,n)})$ entonces x_1 es también solución.

Ejemplo
$3x \equiv 9\,(7)$
$3x \equiv 2\,(7)$
y se cumple que $mcd(3, 7)|2$
por tanto $3x - 7q = 2$ y $x = 3$ y $q = 1$ son solución
por lo que $x \equiv 3\,(7)$

Teorema. *La ecuación lineal congruencial* $ax \equiv b\,(n)$ *donde* $d = (a, n)$ *y* $d|b$ *tiene exactamente* d *soluciones*

Demostración

Ya se observó que la ecuación de congruencia lineal es equivalente a la ecuación lineal Diofantina $ax - ny = b$ y esta ecuación se resuelve si $(a, n)|b$ y como $d = (a, n)$ entonces $d|b$.

Esta ecuación tiene entonces las soluciones $x = x_0 + \frac{n}{d}t$ $y = y_0 + \frac{a}{d}t$ donde x_0 y y_0 es una solución de la ecuación Diofantina.

Si se considera $t = 0, 1, 2, \ldots, d-1$ entonces
x_0, $x_0 + \frac{n}{d}$, $x_0 + \frac{2n}{d}$,$\ldots$, $x_0 + \frac{(d-1)n}{d}$ son soluciones.

Ahora hay que verificar que estas d soluciones son incongruentes entre ellas y cualquier otra fuera de ellas es congruente con alguna de ellas.

Verifiquemos lo primero, si asumimos que no se cumple entonces
$x_0 + \frac{t_1 n}{d} \equiv x_0 + \frac{t_2 n}{d}\,(n)$ con $0 \leq t_1 < t_2 \leq d-1$
entonces se tiene que $\frac{t_1 n}{d} \equiv \frac{t_2 n}{d}\,(n)$
como se tiene que $(\frac{n}{d}, n) = \frac{n}{d}$ luego se llega a que $t_1 \equiv t_2\,(d)$
y esto implica que $d|t_2 - t_1$ pero esto es una contradicción pues se cumple que $0 < t_2 - t_1 < d$

Ahora hay que demostrar que cualquier otra solución $x_0 + \frac{n}{d}t$
es congruente módulo n con una de las soluciones x_0, $x_0+\frac{n}{d}$,$\ldots$, $x_0+\frac{(d-1)n}{d}$
Por el Algoritmo de la División $t = qd + r$ donde $0 \leq r \leq d-1$
entonces $x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r) = x_0 + nq + \frac{n}{d}r$
por tanto $x_0 + \frac{n}{d}t \equiv x_0 + nq + \frac{n}{d}r \equiv x_0 + \frac{n}{d}r\,(n)$
y $x_0 + \frac{n}{d}r$ es una de las soluciones de referencia

Ejemplo

$18x \equiv 30(42)$ como $(18, 42) = 6$ y $6|30$ entonces la ecuación
tiene exactamente 6 soluciones incongruentes entre ellas.
Como una solución de la ecuación es 4 entonces las 6 soluciones
son de la forma $x \equiv 4 + t\frac{42}{6} \equiv 4 + 7t\,(42)$ con $t = 0, 1, \ldots, 5$
lo que es $x \equiv 4, 11, 18, 25, 32, 39\,(42)$

Corolario. *Si $mcd(a, n) = 1$ entonces la ecuación lineal congruencial $ax \equiv b\,(n)$ tiene una única solución módulo n*

Teorema. ***Teorema Chino del Resto*** *Sean $n_1, n_2, \ldots, n_k$ enteros positivos primos relativos 2 a 2, entonces el sistema de ecuaciones de congruencia lineal:*
$x \equiv a_1\,(n_1)$
$x \equiv a_2\,(n_2)$
$\ldots\ldots$
$\ldots\ldots$
$x \equiv a_k\,(n_k)$
tiene una única solución módulo $(n_1 * n_2 * \ldots * n_k)$

Demostración

Se tiene $p = n_1 * n_2 * \ldots * n_k$ y $p_j = \frac{p}{n_j}$ con $1 \leq j \leq k$
como los n_j son primos relativos 2 a 2 entonces $(n_j, p_j) = 1$
por tanto existen r_j y s_j tales que $r_j n_j + s_j p_j = 1$ luego $s_j p_j = -r_j n_j + 1$
y con ello $p_j x \equiv 1\,(n_j)$ tiene solución única y si llamamos s_j a esa solución
se tiene que $p_j s_j \equiv 1\,(n_j)$
pero también se sabe que para $i \neq j$ se tiene que $p_j s_j \equiv 0\,(n_i)$
entonces si se conforma $A = \sum_{i=1}^{k} a_i p_i s_i$ se tiene que $A \equiv a_i\,(n_i)$
Ahora hay que probar la unicidad de la solución,
o sea que todas las soluciones son congruentes entre ellas.
Asumamos que hay dos soluciones x y y diferentes,
entonces se debe cumplir que
$x \equiv a_i\,(n_i)$
$y \equiv a_i\,(n_i)$
esto implica que $x - y \equiv 0\,(n_i)$
ahora como todos los n_i son primos relativos entonces $n_1 n_2 \ldots n_k | x - y$
luego $x \equiv y\,(n_1 n_2 \ldots n_k)$
por tanto las soluciones son congruentes entre ellas, como

Ejemplo

Encuentra un número que deja resto 2,3,2 cuando se divide por 3, 5 y 7 respectivamente.

Se tiene el sistema:
$x \equiv 2\,(3)$
$x \equiv 3\,(5)$
$x \equiv 2\,(7)$
Entonces se tiene $p = 3 * 5 * 7 = 105$
Luego $p_1 = 105/3 = 35$, $p_2 = 105/5 = 21$ y $p_3 = 105/7 = 15$
A partir de esto se tienen las ecuaciones de congruencias lineal
$35x_1 \equiv 1\,(3)$ donde $x_1 = 2$ es solución
$21x_2 \equiv 1\,(5)$ donde $x_2 = 1$ es solución
$15x_3 \equiv 1\,(7)$ donde $x_3 = 1$ es solución
Luego $A = a_1 p_1 x_1 + a_2 p_2 x_2 + a_3 p_3 x_3 = 2*35*2+3*21*1+2*15*1 = 233$
Entonces $A = 233 \equiv 23\,(105)$