Conferencia 5 - Sistemas Residuales

December 7, 2024

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 $d = (a,)$ 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, $x_0 + \frac{n}{d}$, $x_0 + \frac{2n}{d}$,..., $x_0 + \frac{(d-1)n}{d}$ 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 $0 < t2 - t1 < d$

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, $x_0+\frac{n}{d}$,..., $x_0+\frac{(d-1)n}{d}$

Por el Algoritmo de la División $t = qd + r$ donde $o \leq r \leq d - 1$

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 incongüentes 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 $A = 233 \equiv 23\,(105)$

Definición. *Si $a \in \mathbb{Z}$ tal que $(a, n) = 1$ entonces la solución de la ecuación de congruencia lineal $ax \equiv 1\,(n)$ se llama inverso de a módulo n y se denota $\bar{a}$ y se dice que a es inversible módulo n*

Ejemplo

$7x \equiv 1\,(31)$

$x \equiv 9\,(31)$
$\bar{7} \equiv 9\,(31)$

Note que se cumple que $\frac{a}{b} \equiv a\bar{b}\,(n)$
Demostración
Si $b\bar{b} \equiv 1\,(n)$ entonces $ab\bar{b} \equiv a\,(n)$
ahora como $(b,n)=1$ entonces $a\bar{b} \equiv \frac{a}{b}\,(n)$ que es lo mismo que $\frac{a}{b} \equiv a\bar{b}\,(n)$

Note también que el inverso módulo n es único
Demostración
Como $a\bar{a} \equiv 1\,(n)$ entonces $a\bar{a}b \equiv b\,(n)$
luego $x = \bar{a}b$ es solución de la ecuación $ax \equiv b\,(n)$ tal que $(a,n)=1$
y, por tanto, esta solución es única

Por otra parte, si se hace $n = p$ con p primo, $a \in \mathbb{Z}$, $(a,p)=1$
entonces, por el **Pequeño Teorema de Fermat**, $a^{p-1} \equiv 1\,(p)$
por lo que $\bar{a} = a^{p-2}$ pues $aa^{p-2} = a^{p-1} \equiv 1\,(p)$
luego como $ax \equiv b\,(p)$ entonces $x \equiv a^{p-2}b\,(p)$

Proposición. *Sea $n \in \mathbb{Z}$, si a es primo relativo con n (o sea, $mcd(a,n)=1$) entonces existe un entero b tal que $ab \equiv 1\,(n)$. Recíprocamente, si a y b son enteros tales que $ab \equiv 1\,(n)$ entonces a y n no tienen factores en común (o sea, $mcd(a,n)=1$)*

Teorema. ***Teorema de Wilson***. *Sea p entero mayor que 1, p es primo si y solo si $(p-1)! \equiv -1\,(p)$*

Demostración
Demostremos primero que si $p|(p-1)!+1$ entonces p es primo
Asumamos que existe d tal que $d|p$ (o sea, p no es primo) con $1 < d < p$
por tanto $d \leq p-1$ por lo que $d|(p-1)!$
pero como $d|(p-1)!+1$ entonces $d|1$ por lo que $d=1$
lo que contradice a $1 < d < p$ y, por tanto, p debe ser primo

Demostremos ahora que si p es primo entonces $p|(p-1)!+1$
Es fácil verificar que el teorema se cumple para $p = 2, 3$
entonces tomemos $p > 3$
Un $SRC(p) = \{0, 1, 2, \ldots, p-1\}$ y si se tiene $a \in SRC(p)$
entonces si $(a,p)=1$ se tendría que $ax \equiv 1\,(p)$ tiene solución y es única

Luego, con excepción del 0, para todo elemento de SRC(p) se tiene que hay un número del propio conjunto que ambos multiplicados dejan resto 1.

Ahora, si a es una solución de $ax \equiv 1\,(p)$ se tendría que $p|a^2-1$

o lo que es lo mismo $p|(a-1)(a+1)$ y como $a \in SRC(p)$
entonces a es 1 o a es $p-1$
Entonces para el conjunto $S = \{2, \ldots, p-2\}$ si b es solución de $ax \equiv 1\,(p)$
tal que $a \neq b$ y $a, b \in S$ luegp $2 * 3 * \ldots * (p-2) = (p-2)! \equiv 1\,(p)$
y esto es lo mismo que $(p-1)! \equiv p-1\,(p)$ y como $p-1 \equiv -1\,(p)$
entonces $(p-1)! \equiv -1\,(p)$

Definición. *Sea $n \in \mathbb{Z}_+$, la **Función de Euler** que se denota $\varphi(n)$ representa el número de enteros positivos menores o iguales que n primos relativos con n. O sea $\varphi(n) = |\{d\,|1 \leq d \leq n, (d,n) = 1\}|$.*

Para 1 se define $\varphi(1) = 1$

Definición. *Se llama **Sistema Residual Reducido módulo n** (SRR(n)) a un conjunto de $\varphi(n)$ enteros positivos incongruentes módulo n que son primos relativos con n*

O sea, dado un natural positivo n, se dice que un conjunto SRR es un **Sistema Residual Reducido módulo n** si cumple lo siguiente:

1. SRR posee $\varphi(n)$ elementos
2. para cada $a \in SRR$ se cumple $(a, n) = 1$
3. los elementos de SRR son incongruentes módulo de n entre si. O lo que es lo mismo, si $a, b \in SRRR$ y $a \neq b$ entonces $a \not\equiv b\,(n)$

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

Demostración
Supongamos que $\{ka_1, ka_2, \ldots, ka_{\varphi(n)}\}$ no es un SRR(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 $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$ tampoco es un SRR(n),
por tanto, por contrarecíproco, si $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$ es un SRR(n)
entonces $\{ka_1, ka_2, \ldots, ka_{\varphi(n)}\}$ también lo es

Teorema. *$\varphi(p) = p-1$ si y solo si p es primo*

Demostración
Si p es primo entonces significa que todo entero positivo menor que él es primo relativo con él, por tanto $\varphi(p) = p-1$

Ahora, si $\varphi(p) = p-1$ y p es compuesto entonces $p = qr$ con $1 < q \leq r < p$ por lo qué habría al menos dos números enteros positivo, además del propio p, que no serían primos relativos con p por lo que $\varphi(p) \leq p-3$, lo que es una contradicción y, por tanto, p es primo

Teorema. *Si p es primo y $k > 0$ entonces $\varphi(p^k) = p^k - p^{k-1}$*

Demostración

Para cualquier número n se tiene que $(n, p^k) = 1$ si y solo si $p \nmid n$. Ahora, entre 1 y p^k hay p^{k-1} enteros que son divisibles por p y que, por tanto. no son primos relativos con p^k. Estos serían $p, p^2, p^3, \ldots, p^{k-1}p$. Luego, el conjunto $\{1, 2, 3, \ldots, p^k$ contendría $p^k - p^{k-1}$ enteros que son primos relativos con p^k y, por tanto, por definición, $\varphi(p^k) = p^k - p^{k-1}$

Teorema. ***Teorema de Euler*** *Sean $a, n \in \mathbb{Z}$, $n > 0$ y $(a, n) = 1$ entonces $a^{\varphi(n)} \equiv 1\,(n)$*

Demostración

Sea $\{n_1, n_2, \ldots, n_{\varphi(n)}\}$ un SRR(n), entonces $\{an_1, an_2, \ldots, an_{\varphi(n)}\}$
con $a \in \mathbb{Z}$ tal que $(a, n) = 1$ es también un SRR(n), luego se cumple
$(an_1)(an_2)\ldots(an_{\varphi(n)}) \equiv n_1 n_2 \ldots n_{\varphi(n)}\,(n)$
$a^{\varphi(n)} n_1 n_2 \ldots n_{\varphi(n)} \equiv n_1 n_2 \ldots n_{\varphi(n)}\,(n)$
pero como $\forall(i) 1 \leq i \leq \varphi(n)$ $(n_i, n) = 1$
entonces $a^{\varphi(n)} \equiv 1\,(n)$