1. Aritmética Modular

Definicion 1.1. Sean a y b enteros y m un entero positivo. Decimos que a es congruente con b modulo m y se representa por $a \equiv b (\operatorname{mod} m)$. Si m divide a $a - b$, es decir $m | (a - b)$. Si a no es congruente con b modulo m es decir $a \not\equiv b (\operatorname{mod} m)$

Ejemplo: $8 \equiv 2 (\operatorname{mod} 3)$?

Veamos si $3 | (8 - 2)$ es decir $3 | 6$
Es cierto que $3 | 6$ porque $6 = 3 \cdot 2$
$\therefore 8 \equiv 2 (\operatorname{mod} 3)$

Ejemplo: $10 \equiv 4 (\operatorname{mod} 8)$?

$$\begin{aligned} 10 \not\equiv 4 (\operatorname{mod} 8) &\Longleftrightarrow 8 | (10 - 4) \\ &\Longleftrightarrow 8 | 6 \\ &\Longleftrightarrow 6 = 8 \cdot c \\ &\Longrightarrow c \notin \mathbb{Z} \end{aligned}$$

$\therefore 10 \not\equiv 4 (\operatorname{mod} 8)$

Teorema 1.2. $a, b \in \mathbb{Z} \land m \in \mathbb{Z}^+ \land a \equiv b (\operatorname{mod} m) \Longleftrightarrow a \operatorname{mod} m = b \operatorname{mod} m$

Prueba:

1. $a \equiv b (\operatorname{mod} m) \Longrightarrow a \operatorname{mod} m = b \operatorname{mod} m$

   Supongamos que $a \equiv b (\operatorname{mod} m)$, es decir $m | (a - b)$, es decir

   $$a - b = mk; \quad k \in \mathbb{Z}$$

   Ahora expresamos a y b en términos de division en m

   $a = mq + r; \quad q \in \mathbb{Z}; \quad 0 \leq r < m$
   $b = mp + s; \quad p \in \mathbb{Z}; \quad 0 \leq s < m$

   Restamos a y b

   $$\begin{aligned} a - b &= (mq + r) - (mp + s) \\ &= mq + r - mp - s \\ &= mq - mp + r - s \\ &= m(q - p) + (r - s) \end{aligned}$$

   Por hipótesis $a - b = mk$, entonces

   $$\begin{aligned} m(q - p) + (r - s) &= mk \\ r - s &= mk - m(q - p) \\ r - s &= m(k - q + p) \end{aligned}$$

   Como $0 \leq r < m \land 0 \leq s < m$, entonces $-m < r - s < m$

   Como $r - s$ debe ser múltiplo de m entonces $r - s = 0$. Ya que 0 es el único múltiplo de m ente $-m$ y m

   Ahora $r - s = 0 \Longrightarrow r = s$

   $\therefore a \operatorname{mod} m = r = s = b \operatorname{mod} m$
2. $a \operatorname{mod} m = b \operatorname{mod} m \Longrightarrow a \equiv b (\operatorname{mod} m)$

   Si $a \operatorname{mod} m = b \operatorname{mod} m$ entonces a y b darán el mismo resto al dividirlos por m. Por lo tanto $a = q_1 m + r \land b = q_2 m + r$

   Restamos a y b

   $$\begin{aligned} a - b &= (q_1 m + r) - (q_2 m + r) \\ &= q_1 m + r - q_2 m - r \\ &= q_1 m - q_2 m \\ &= (q_1 - q_2) m \end{aligned}$$

   Por lo tanto $m | (a - b)$
   $\therefore a \equiv b (\operatorname{mod} m)$

□

Ejemplo: $8 \equiv 2 (\operatorname{mod} 3)$

$8 \operatorname{mod} 3 = \boxed{2}$ porque $8 = 3 \cdot 2 + \boxed{2}$
$2 \operatorname{mod} 3 = \boxed{2}$ porque $2 = 3 \cdot 0 + \boxed{2}$

En efecto $8 \operatorname{mod} 3 = 2 \operatorname{mod} 3$

Teorema 1.3. $a, b, c, d \in \mathbb{Z} \land m \in \mathbb{Z}^+ \land a \equiv b (\operatorname{mod} m) \land c \equiv d (\operatorname{mod} m) \Longrightarrow a + c \equiv (b + d) (\operatorname{mod} m) \land ac \equiv (bd) (\operatorname{mod} m)$

Prueba: Supongamos que $a \equiv b (\operatorname{mod} m) \land c \equiv d (\operatorname{mod} m)$ entonces $m | (a - b) \land m | c - d$ es decir:

$a - b = mk; \quad k \in \mathbb{Z}$
$c - d = mp; \quad p \in \mathbb{Z}$

Luego $a = mk + b \land c = mp + d$

1. Sumando las igualdades

   $$\begin{aligned} a + c &= mk + b + mp + d \\ &= (b + d) + mk + mp \\ &= (b + d) + m(k + p) \end{aligned}$$

   Como $k, p \in \mathbb{Z}$ entonces $k + p \in \mathbb{Z}$ llamemos $n = k + p$

   Por lo tanto

   $$\begin{aligned} a + c &= (b + d) + mn \\ (a + c) - (b + d) &= mn \end{aligned}$$

   Osea $m | (a + c) - (b + d)$

   $\therefore (a + c) \equiv (b + d) (\operatorname{mod} m)$
2. Multiplicando las igualdades

   $$\begin{aligned} ac &= (mk + b)(mp + d) \\ &= m^2 kp + mkd + mpb + bd \\ &= m(mkp + kd + pb) + bd \end{aligned}$$

   Como $m, k, p, d, b \in \mathbb{Z}$ entonces $mkp + kd + pb \in \mathbb{Z}$ llamemos $n = mkp + kd + pb$

   Por lo tanto

   $$\begin{aligned} ac &= mn + bd \\ ac - bd &= mn \end{aligned}$$

   Osea $m | ac - bd$

   $\therefore ac \equiv bd (\operatorname{mod} m)$

□

1.1. Aplicaciones de las convergencias

1.1.1. Funciones de dispersion

Memoria de un computador $\leftarrow$ Información

Por ejemplo la universidad debe guardar la información de todos los estudiantes, guarda sus datos personales y academes. Como hacer para poder acceder a la información de cada estudiantes de forma efectiva?

Para esto se usan las funciones de dispersion:

La información se almacena en ficheros cada uno de ellos se localiza usando una clave, que identifica de forma única el fichero de cada estudiante. En particular la identificación puede ser el código estudiantil. En particular la identificación puede ser el código estudiantil. Una función de dispersion h asigna una posición de memoria $h(k)$ al fichero que tiene a k como clave. Existen muchas funciones de dispersion, una de ellas es $h(k) = k \operatorname{mod} m$ donde m es el numero de posiciones de memoria existentes.

$h(k) = k \operatorname{mod} m$. Residuo de dividir k por m

Ejemplo: $m = 100$ (cantidad maxima de posiciones de memoria)

- $k_1 = 20251167000$ Código estudiantil
  $h(k_1) = 20251167000 \operatorname{mod} 100 = \boxed{0}$
  $\therefore$ al estudiante de código k_1 se le asigna la posición de memoria 0
- $k_2 = 20251167026$ Código estudiantil
  $h(k_2) = 20251167026 \operatorname{mod} 100 = \boxed{26}$
  $\therefore$ al estudiante de código k_2 se le asigna la posición de memoria 26
- $k_3 = 20251167100$ Código estudiantil
  $h(k_3) = 20251167100 \operatorname{mod} 100 = \boxed{0}$
  Como la posición de memoria 0 se encuentra ocupada por k_1 se le asigna la siguiente, osea 1
  $\therefore$ al estudiante de código k_3 se le asigna la posición de memoria 1

«Nota: Puede ocurrir que dos códigos estudiantiles dejen el mismo residuo al dividirse por m. En este caso se dice que ha ocurrido una colisión. Una forma de solucionar esta situación es asignar al código que genera repetición del residuo, la siguiente posición de memoria que esté libre en ese momento.»

1.1.2. Números pseudoaleatorios (Método de congruencia lineal)

Para generar números pseudoaleatorios usaremos el método de congruencia lineal. Elegimos cuatro números enteros:

- El modulo m
- El multiplicador a
- El incremento c
- La semilla x_0

Que satisfaga $2 \leq 1 < m, 0 \leq c < m, 0 \leq x_0 < m$

Generamos una sucesión de números pseudoaleatorios x_n, $0 \leq n < m$ así: aplicando reiteradamente la congruencia:

$$x_{n+1} = (a x_n + c) \operatorname{mod} m$$

Ejemplo: $m = 8; \quad a = 5; \quad c = 3; \quad x_0 = 2$

- $x_1 = (5x_0 + 3) \operatorname{mod} 8 = (5 \cdot 2 + 3) \operatorname{mod} 8 = 13 \operatorname{mod} 8 = \boxed{5}$
- $x_2 = (5x_1 + 3) \operatorname{mod} 8 = (5 \cdot 5 + 3) \operatorname{mod} 8 = 28 \operatorname{mod} 8 = \boxed{4}$
- $x_3 = (5x_2 + 3) \operatorname{mod} 8 = (5 \cdot 4 + 3) \operatorname{mod} 8 = 23 \operatorname{mod} 8 = \boxed{7}$
- $x_4 = (5x_3 + 3) \operatorname{mod} 8 = (5 \cdot 7 + 3) \operatorname{mod} 8 = 38 \operatorname{mod} 8 = \boxed{6}$
- $x_5 = (5x_4 + 3) \operatorname{mod} 8 = (5 \cdot 6 + 3) \operatorname{mod} 8 = 33 \operatorname{mod} 8 = \boxed{1}$
- $x_6 = (5x_5 + 3) \operatorname{mod} 8 = (5 \cdot 1 + 3) \operatorname{mod} 8 = 2 \operatorname{mod} 8 = \boxed{2}$

Aquí como volvimos a llegar a la semilla $x_0 = x_6$ se repetiría, por lo tanto nuestra sucesión de números aleatorios es: $\{5, 4, 7, 6, 1, 2\}$

1.1.3. Cristología

Las congruencias tienen muchas aplicaciones, en particular en las ciencias de la computación. Una de ellas es la cristología o criptografía, que es el estudio de los mensajes secretos

Ejemplo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
14	15	16	17	18	19	20	21	22	23	24	25	26	

Encriptar el mensaje «La próxima semana tendremos vacaciones»
Usando la numeración dada el mensaje es: «11 0 16 18 15 24 8 12 0 19 4 12 0 13 0 20 4 13 3 18 4 12 15 19 22 0 2 0 2 8 15 13 4 19»

Este método de encriptación se basa en reemplazar cada uno de los números del mensaje por: $f(p) = (p + 3) \operatorname{mod} 27$

Así, el mensaje encriptado es: «14 3 19 21 18 0 11 15 3 22 7 15 3 16 3 23 7 16 6 21 7 15 18 22 25 3 5 3 5 11 18 16 7 22»

Para recuperar el mensaje original del mensaje encriptado debemos usar la función inversa de f

$f^{-1}(p) = (p - 3) \operatorname{mod} 27$ donde $0 \leq p < 27$

Se puede generalizar este método, se puede desplazar k lugares en lugar de 3 letras en el alfabeto; es decir $f(p) = (p + k) \operatorname{mod} 27$. A este método se le llama cifrado por translación.
Y se descifra con la función inversa $f^{-1}(p) = (p - k) \operatorname{mod} 27$. A este proceso se llama descifrado o decodificación.