Curso

Aritmética modular ($n \geq 2$)

$(\mathbb{Z}_n, +)$ cíclico

$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, \dots, \widehat{n-1}\}$ $\quad \hat{k} = \{x \in \mathbb{Z} : x \text{ es congruente a } k \text{ módulo } n\}$

$\hat{k} = \{y \in \mathbb{Z} : y \equiv k \pmod{n}\}$

$\hat{2} + \hat{2} = \widehat{2+2}$

$\hat{2} \cdot \hat{2} = \widehat{2 \cdot 2}$

$(\mathbb{Z}, +)$ grupo conmutativo de orden $\hat{0}$

$\hat{0}$: conjunto bien definido

$-\hat{2} = \widehat{-2}$ opuesto bien definido

$-\hat{2} + \hat{2} = \hat{0} + \hat{0} = \hat{0}$.

$(\mathbb{Z}, +, \cdot)$ anillo conmutativo

Con un neutro

$\hat{1}$: el neutro

$\hat{2}^{-1}$: conjunto (nunca) no $\hat{2}$ bien def. "divisor nulo"

$\hat{2}^{-1} \cdot \hat{3} = \hat{2} \cdot \hat{2} = \hat{4}$

Ej: $\mathbb{Z}_5 : \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}\}$ $\rightarrow$ representado

$\hat{1} + \hat{0} = \hat{1}$

$-\hat{3} = \widehat{-3} = \hat{2}$ $\quad \hat{2} + \hat{3} = \hat{5} = \hat{0}$

$-\hat{2} = \widehat{-2} = \hat{3}$ $\quad \hat{3} + \hat{2} = \hat{5} = \hat{0}$

$\hat{2}^{-1} \cdot \hat{3} = \hat{3} \cdot \hat{2}^{-1} = \hat{1} \cdot \hat{3} = \hat{3}$ pf. $\hat{2} \cdot \hat{3} = \hat{5} = \hat{0} = \hat{1} \cdot \hat{0}$

$\hat{2}^{-1} \cdot \hat{3} = \hat{0}$

$\hat{2}^{-1} \cdot \hat{0}$ pf. $\hat{2} \cdot \hat{0} = \hat{0} \cdot \hat{3} = \hat{3} \cdot \hat{2} = \hat{0}$

$\hat{2}^{-1} \cdot \hat{2} = \hat{1} \cdot \hat{2} = \hat{2} \cdot \hat{3} = \dots$

Ej: $\mathbb{Z}_{20}$ $\quad \hat{2}^{-1} \cdot \hat{3} = \hat{2} \cdot \hat{2} = \hat{4}$, $\hat{2}\hat{2}^{-1} \cdot \hat{4}$

$\hat{2}\hat{2}^{-1}$ no existe

Def: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \exists x^{-1} = \mathbb{Z}_n\}$ $\rightarrow$ grupo multiplicativo

$\hookrightarrow$ $\mathbb{Z}_n$ anillo

Teorema: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid (\text{com}(x,n)) = 1\}$

Obs1: base $x \cdot y$ pm $\Rightarrow U(\mathbb{Z}_n) : \mathbb{Z}_n \setminus \{\hat{0}\}$

Obs2: base $a \in U(\mathbb{Z}_n) \Rightarrow \exists y \in \mathbb{Z}_n$, $y \neq \hat{0}$ al: $xy = \hat{0}$.

$\hookrightarrow$ no existe xy no bien x bien

Ej: $U(\mathbb{Z}_5) : \{\hat{1}, \hat{2}, \hat{3}, \hat{4}\}$ $\quad \hat{2}^{-1} \cdot \hat{3} = \hat{3} \cdot \hat{2}^{-1} = \hat{3} \cdot \hat{3} = \hat{4}$

$\hookrightarrow$ $\forall \hat{x} \in U(\mathbb{Z}_n)$ $\quad \hat{x} \cdot \hat{0} = \hat{0} \cdot \hat{x} = \hat{0}$ divisor x bien bien

Función de Euler $\varphi : \mathbb{Z} \to \mathbb{Z}$

Ej: $5x + 2 = 1$ $\quad \mathbb{Z}_n$

$5x + 2 = 1 \Rightarrow 5x + 1 = 3^2 \cdot 3 \Rightarrow x = 80 \cdot 2 = 2$

Ej: $3x - 5 = 1$ $\quad \mathbb{Z}_{13}$

$3x - 1 = 3^2 \cdot 3 \Rightarrow x = 3 \cdot 2 = 6$

Ej: $2x - 1 = 0 \Rightarrow \mathbb{Z}_5$ $\quad$ Prueba por tanteo

$2x = 5$ $\quad$ $\begin{array}{c|ccccc} x & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline 2x & 0 & 2 & 4 & 0 & 2 & 4 \end{array}$

2^{-1} no existe $\mathbb{Z}_5$ $\quad$ $\Rightarrow$ $\hat{2} = \hat{4}$

Sistema Lineales

Ej: $\begin{cases} 2x + y = 3 \\ 4x - 3y = 1 \end{cases}$ $\in \mathbb{Z}_7$ $\quad A = \begin{pmatrix} 2 & 1 \\ 4 & -3 \end{pmatrix}$

$\det A = -4 - 5 = -9 = -2 = \text{det}(U(\mathbb{Z}_7))$

$\Rightarrow$ bien inv

$\begin{cases} 2x + y = 3 \mid \cdot 2 \\ 4x - 3y = 1 \end{cases}$ $\quad$ $\begin{array}{l} \text{no inv} \Rightarrow \text{det} = 0 \\ \begin{cases} 2x + y = 3 \\ 2x - 3y = 2 \end{cases} \end{array}$ $\Rightarrow$ no sol $\quad$ $\boxed{\text{sol}}$

$2 \cdot 0 + 1 \cdot 3 = 3$

$4 \cdot 0 - 3 \cdot 3 = 1 \neq 2$

Ej: $\begin{cases} 3x - 2y = 1 \\ x + y = 2 \end{cases}$ $\in \mathbb{Z}_4$ $\quad A = \begin{pmatrix} 3 & -2 \\ 1 & 1 \end{pmatrix}$ $\det A = 5 \notin U(\mathbb{Z}_4)$

$\begin{cases} 3x - 2y = 1 \\ 2x + y = 1 \end{cases}$ $\Rightarrow$ $\begin{array}{l} 6x - 5 = 1 \Rightarrow x = 1 \text{ bien} \\ x \in \{0, 1, 2, 3\} \end{array}$

$H = \begin{cases} x = 0 \Rightarrow -2 = 1 \\ x = 1 \Rightarrow 3 - 2y = 1 \Rightarrow y = 1 \\ x = 2 \Rightarrow 6 - 2y = 1 \Rightarrow y = 2 \\ x = 3 \Rightarrow 9 - 2y = 1 \Rightarrow y = 4 \end{cases}$ $\quad$ $\begin{array}{l} x = 0 \Rightarrow 3 \cdot 0 - 2 \cdot 0 = 1 \cdot 0 \\ x = 1 \Rightarrow 3 \cdot 1 - 2 \cdot 1 = 1 \cdot 1 \\ x = 2 \Rightarrow 3 \cdot 2 - 2 \cdot 2 = 1 \cdot 2 \\ x = 3 \Rightarrow 3 \cdot 3 - 2 \cdot 4 = 1 \cdot 3 \end{array}$

$S = \{(1,0), (1,1), (1,2), (1,3), (1,4)\}$

Ec de grado ≤ 2

Ej: $x^2 + 5x + 3 = 2 \in \mathbb{Z}_{10}$ $\quad$ $\begin{array}{c|ccccccc} x & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline x^2 & 0 & 1 & 4 & 2 & 3 & 2 & 3 \end{array}$

$\Delta = 25 - 12 = 13 = 16$

$\sqrt{16} = \pm 4 = 0$ $\quad$ $\sqrt{-1} \notin \mathbb{Z}_{10} = \{\pm 4\}$

Ej: $x^2 + 5x + 3 = 2 \in \mathbb{Z}_{10}$

$x^2 - 5x + 1 = 0$

$\Delta = 25 - 4 = 5$

$\sqrt{5} \notin \mathbb{Z}_{10}$

Basta con $6 + 5 = 1$ $\quad x_1 = (5 + 6) \cdot 2^{-1} = 6 \cdot 6 = 36 = 2$

$x_2 = (5 - 6) \cdot 6 = -6 \cdot 6 = -36 = 4$

Basta con $\sqrt{5} = 16 \Rightarrow x_1 = (5 + 16) \cdot 2^{-1} = \frac{21 \cdot 6}{2} = 63 = 2$

$x_2 = (5 - 16) \cdot 2^{-1} = -11 \cdot 6 = -66 = -22 = 8 = -2 = 8$.

$x \in \{2, 8\}$

Cifrado simple: Cesar, afín, Hill

Cifrado $\quad$ flujo (stream cipher) $\rightarrow$ del mensaje se cifra en cada clave

$\quad$ $\rightarrow$ bloque (block cipher) $\rightarrow$ cifra a través de bloque de tamaño clave

$\quad$ $\rightarrow$ Ej bloque: (block cipher) $\rightarrow$ cifra a través de bloque clave

$\quad$ flujo padding $\rightarrow$ relleno los grupos de bloques

$\quad$ bloque padding $\rightarrow$ hacer bloque con mismo longitud (ej: bits bloque tamaño)

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

Lo de bajo es bueno en $\mathbb{Z}_{26} = \{0, 1, \dots, 25\}$ $\rightarrow$ dar un texto en un cuerpo, más 1 letra en un grupo

Abanico $\begin{array}{c} \text{Lu} \\ \text{Ma} \\ \text{Mi} \end{array}$ $\begin{array}{c} 1 \\ 2 \\ 3 \end{array}$ $\Rightarrow$ $\mathbb{Z}_{29}$ $\quad$ 1 letra por mes. $(U(\mathbb{Z}_{29})) = \mathbb{Z}_{29} \setminus \{0\}$

Cifrado Cesar

Función de cifrado: $\text{cod} : \text{mensaje} \to \text{clave} \in \mathbb{Z}_{29}$

Función de descifrado: $\text{mensaje} : \text{cod} \to \text{clave}$

Ej: $\text{mensaje} = \text{CRIPTO}$ $\quad [\text{mensaje}] = [2, 17, 8, 15, 19, 14]$ $\xrightarrow{\text{clave}=17}$

$\text{clave} = 17$

$\rightarrow [19, 34, 25, 32, 36, 31]$ $\xrightarrow{\text{mod } 29}$ $[19, 5, 25, 3, 7, 2] \rightarrow$ TFZDHC

Ej Skrom:

Longitud Mensaje $b = 4$

$\text{mensaje} = \text{CRIPTO} \Rightarrow$ CRIP

TOL!

$\rightarrow$ padding random

$\text{clave}_1 = 15$

$\text{clave}_2 = 8$

$[CRI, P] \rightarrow [2, 17, 8, 15] \xrightarrow{+\text{clave}_1} [17, 32, 23, 30] \xrightarrow{\text{mod } 29} [17, 2, 23, 1] \rightarrow RDXB$

$[T, O, R, L] \rightarrow [19, 14, 17, 28] \xrightarrow{+\text{clave}_2} [27, 22, 25, 36] \xrightarrow{\text{mod } 29} [27, 22, 25, 7] \rightarrow WZH$

CRIPTO! $\rightarrow$ RDXB.WZH

Descifrado

$[R, D, X, B] \rightarrow [17, 3, 23, 1] \xrightarrow{-\text{clave}_1} [2, -12, 8, -14] \xrightarrow{\text{mod } 29} [2, 17, 8, 15] \rightarrow \text{CRIP}$

$[., W, Z, H] \rightarrow [27, 22, 25, 7] \xrightarrow{-\text{clave}_2} [19, 14, 17, -1] \rightarrow [19, 14, 17, 28] \rightarrow \text{TOL!}$

Cifrado afín: flujo

Ec de cifrado: $\text{cod} : \text{mensaje} \cdot \text{clave}_1 + \text{clave}_2$

Ec de descifrado: $\text{mensaje} = (\text{cod} - \text{clave}_2) \cdot \text{clave}_1^{-1}$

Ej: $\text{mensaje} = \text{CRIPTO}$ $\quad [\text{mensaje}] = [2, 17, 8, 15, 19, 14]$ $\xrightarrow{\text{clave}_1 = 4}$

$\text{clave}_2 = 12$

$\rightarrow [19, 34, 25, 32, 36, 31]$ $\xrightarrow{\text{mod } 29}$ $[19, 5, 25, 3, 7, 2] \rightarrow$ TFZDHC

Ej Skrom:

Longitud Mensaje $b = 4$

$\text{mensaje} = \text{CRIPTO} \Rightarrow$ CRIP

TOL!

$\rightarrow$ padding random

$\text{clave}_1 = 15$

$\text{clave}_2 = 8$

$[CRI, P] \rightarrow [2, 17, 8, 15] \xrightarrow{+\text{clave}_1} [17, 32, 23, 30] \xrightarrow{\text{mod } 29} [17, 2, 23, 1] \rightarrow RDXB$

$[T, O, R, L] \rightarrow [19, 14, 17, 28] \xrightarrow{+\text{clave}_2} [29, 22, 25, 36] \xrightarrow{\text{mod } 29} [29, 22, 25, 7] \rightarrow WZH$

CRIPTO! $\rightarrow$ RDXB.WZH

Descifrado

$[R, D, X, B] \rightarrow [17, 3, 23, 1] \xrightarrow{-\text{clave}_1} [2, -12, 8, -14] \xrightarrow{\text{mod } 29} [2, 17, 8, 15] \rightarrow \text{CRIP}$

$[., W, Z, H] \rightarrow [27, 22, 25, 7] \xrightarrow{-\text{clave}_2} [19, 14, 17, -1] \rightarrow [19, 14, 17, 28] \rightarrow \text{TOL!}$

Cifrado afín: flujo

Ec de cifrado: $\text{cod} : \text{mensaje} \cdot \text{clave}_1 + \text{clave}_2$

Ec de descifrado: $\text{mensaje} = (\text{cod} - \text{clave}_2) \cdot \text{clave}_1^{-1}$

Ej: $\text{mensaje} = \text{CRIPTO}$ $\quad [\text{mensaje}] = [2, 17, 8, 15, 19, 14]$ $\xrightarrow{\text{clave}_1 = 4}$

$\text{clave}_2 = 12$

$\rightarrow [20, 22, 15, 19, 1, 16] \xrightarrow{\text{mod } 29} \rightarrow \text{UWPOBA}$

$80 : 58 + 22 = 22$

descifrado: $\text{UWPOBA} \rightarrow [20, 22, 15, 19, 1, 16] \xrightarrow{-12, \cdot 4^{-1}} [-56, -70, -21, -19, 72, 16]$

$-12, \cdot 22$

$\cdot (-7)$

$\xrightarrow{\text{mod } 29} [2, 17, 8, 15, 19, 14] \rightarrow \text{CRIPTO}$

$-56 = -58 + 2$

$-70 = -58 - 12 = -12 = 17$

$72 = 58 + 14$

Ej Skrom:

$\text{mensaje} = \text{CRIPTO}$, $b = 4$ $\quad$ fórmula padding

$\Rightarrow$ CRIP, $k1 = 5$, $k2 = 13$ $\rightarrow [2, 17, 8, 15] \xrightarrow{+k1} [21, 36, 23, 30] \rightarrow [21, 7, 23, 30]$

TO, $k3 = 3$, $k4 = 14$

$\rightarrow [19, 14] \xrightarrow{+k3} [19, 17]$

$\rightarrow [21, 7, 23, 30, 19, 17]$

$k4 = 3 + 9 = 9$

$\boxed{\text{VJWL!}}$

$[T, O] \rightarrow [19, 14] \xrightarrow{+k3} [19, 17] \xrightarrow[\text{mod } 29]{} [3, 17] \rightarrow \text{DR}$

$\text{CRIPTO} \rightarrow \text{VJWL!DR}$

Cifrado Hill

Cheia: matriz de cifrado

Ec de cifrado: $\begin{pmatrix} 0 \\ 0 \\ b \end{pmatrix} = \begin{pmatrix} M \\ A \\ T \end{pmatrix} \cdot \begin{pmatrix} M \\ S \\ J \end{pmatrix} + \begin{pmatrix} M \\ A \\ T \end{pmatrix} \in M_3(\mathbb{Z}_{29})$

Ec de descifrado: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = \begin{pmatrix} M \\ A \\ T \end{pmatrix}^{-1} \cdot \begin{pmatrix} 0 \\ 0 \\ b \end{pmatrix}$

Ej: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = \begin{pmatrix} A \\ Z \\ I \end{pmatrix}$, $\quad \text{Mat} = \begin{pmatrix} -1 & 0 & 2 \\ 1 & -1 & 0 \\ -2 & 1 & 0 \end{pmatrix}$

$\begin{pmatrix} A \\ Z \\ I \end{pmatrix} = \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix}$, $\quad \begin{pmatrix} -1 & 0 & 2 \\ 1 & -1 & 0 \\ -2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix} = \begin{pmatrix} 16 \\ -25 \\ 25 \end{pmatrix}$ mod 29 $= \begin{pmatrix} 16 \\ 4 \\ 25 \end{pmatrix} = \begin{pmatrix} Q \\ E \\ Z \end{pmatrix}$

Descifrado: $A = \begin{pmatrix} -1 & 0 & 2 \\ 1 & -1 & 0 \\ -2 & 1 & 0 \end{pmatrix} \in M_3(\mathbb{Z}_{29})$

$\det A = 2 - 4 = -2 = 27 \in U(\mathbb{Z}_{29})$

$27^{-2} = 14$

$A^T = \begin{pmatrix} -1 & 1 & -2 \\ 0 & -1 & 1 \\ 2 & 0 & 0 \end{pmatrix} \longrightarrow A^{T*} = \begin{pmatrix} 0 & 2 & 2 \\ 0 & 4 & 2 \\ -1 & 1 & 1 \end{pmatrix}$

$A^{-1} = (\det A)^{-1} \cdot A^{T*} = 14 \cdot A^{T*} = \begin{pmatrix} 0 & 28 & 28 \\ 0 & 56 & 28 \\ -14 & 14 & 14 \end{pmatrix} = \begin{pmatrix} 0 & -1 & -1 \\ 0 & -2 & -1 \\ -14 & 14 & 14 \end{pmatrix}$

$\begin{pmatrix} M \\ S \\ J \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} 0 \\ 0 \\ b \end{pmatrix} = \begin{pmatrix} 0 & -1 & -1 \\ 0 & -2 & -1 \\ -14 & 14 & 14 \end{pmatrix} \cdot \begin{pmatrix} 16 \\ 4 \\ 25 \end{pmatrix} = \begin{pmatrix} 0 \\ 25 \\ 6 \end{pmatrix} = \begin{pmatrix} A \\ Z \\ G \end{pmatrix}$