2019 - 10 - 07

Aritmética Modular (Continuación)

- Para sacar ventaja de las propiedades de los enteros módulo n ($\mathbb{Z}_n$) es necesario redefinir las operaciones de suma & multiplicación:

- Dados $a, b \in \mathbb{Z}_n$, la <u>suma módulo n</u> se define de la siguiente manera.

⌈ Aritemética Modular ≡ Aritemética de residuos ⌋

$$\boxed{a +_n b \equiv (a+b) \pmod{n}}$$

<u>Ej:</u> $a = 11$ $\quad b = 7$ $\quad$ & $\quad n = 5$

Residuo de 11 & 5

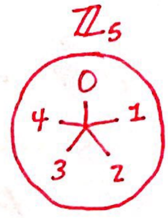
$$11 +_5 7 \equiv 1 +_5 2 \equiv 3$$

Residuo de 7 & 5

Esto equivale a:

$$\underbrace{(11 + 7)}_{\text{La suma habitual de enteros.}} = 18 \equiv_5 3$$

Ej: $a = 11$, $b = 9$, $n = 5$



$$11 +_5 9 \equiv_5 \underbrace{1 +_5 4}_{\frac{5}{5} = 1 + 0} \equiv_5 0$$

$$(11 + 9) = \underbrace{20}_{\frac{20}{5} = 4 + 0} \equiv_5 0$$

▲ De forma similar se define la multiplicación módulo n:

$$\boxed{a \cdot_n b = (a \cdot b)(\mathrm{mod}_n)}$$

▲ Ceasar's shift:

cripto - grafia
oculto escritura
criptología

- Un sistema criptográfico cuyo funcionamiento fue entenderse usando aritmética modular.
- Requiere identificar cada letra del abecedario con uno y sólo uno de los enteros módulo n. En éste ejemplo usarémos mod 26 por tener 26 letras. Por ejemplo:

$$\left.\begin{array}{l} A \rightarrow 0 \\ B \rightarrow 1 \\ C \rightarrow 2 \\ \vdots \\ Z \rightarrow 25 \end{array}\right\} \text{diccionario}$$

Asociada al sistema cryptográfico existe dos funciones:

1) Función encriptación: Ceasar's shift:

$$E(x) = x + \underbrace{d}_{\text{shift}}$$

... en donde $d \in \mathbb{Z}_{26}$

Por ejemplo, si $d \equiv_{26} 3$

A, B, C, ... , Y, Z
↓ ↓ ↓ ↓ ↓
0 1 2 24 25

$\boxed{E(x)}$

3 4 5 ... 1 2
↓ ↓ ↓ ↓ ↓
D E F ... B C

Ej: Para encryptar el mensaje: CAZ usando $\mathbb{Z}$

C A Z

2 0 26

$\boxed{E(x)}$

6 4 3

G E D

Enviamos el mensaje GED:

Función decriptación:

$$D(x) = x - d$$

G E D

6 4 3

$\boxed{D(x)}$

2 0 25

C A Z

<u>Observaciones finales</u>:

- ventaja: implementación es simple.
- desventaja: subseptible al análisis de frecuencias; siempre se repite la misma letra.