LE CONGRUENZE E IL CIFRARIO DI CESARE

Ma la matematica dov'è?

Riprendiamo il primo esempio in cui la chiave è 5

La A in posizione 0 va in posizione $0+5=5$

La B in posizione 1 va in posizione $1+5=6$

....

La S in posizione 16 va in posizione $16+5=21$ ma le posizioni possibili sono solo da 0 a 20 quindi andrà al posto della A, cioè in posizione 0

La T in posizione 17 va in posizione $17+5=22$, andrà al posto della B cioè in posizione 1

La U _____

La V _____

La Z _____

In matematica questo tipo di calcoli rientrano nell'aritmetica modulare o aritmetica dell'orologio.

Il primo ad ideare questa aritmetica fu Gauss

Definizione: Sia n un intero positivo fissato. Due numeri $a, b \in \mathbb{Z}$ sono congrui modulo n se e solo se $a-b$ è multiplo di n .

Espresso in formule $a \equiv b \pmod{n} \leftrightarrow (a-b) = n \cdot h$ con $h \in \mathbb{Z}$

Pensiamo all'orologio :

$$15 \equiv 3 \pmod{12}; \quad 18 \equiv 6 \pmod{12}; \quad 23 \equiv 11 \pmod{12}$$

Completa le seguenti congruenze:

$$14 \equiv \quad \pmod{12}; \quad 16 \equiv \quad \pmod{12}; \quad 21 \equiv \quad \pmod{12}; \quad 17 \equiv \quad \pmod{12}$$

$$26 \equiv \quad \pmod{12}; \quad 29 \equiv \quad \pmod{12}; \quad 33 \equiv \quad \pmod{12}; \quad 27 \equiv \quad \pmod{12}$$

Scrivi 5 numeri che sono congrui a 7 modulo 12:

Possiamo dire che un numero è congruo a 7 modulo 12 quando

Scrivi 5 numeri che sono congrui a 11 modulo 12:

Possiamo dire che un numero è congruo a 11 modulo 12 quando

In generale possiamo dire che tutti i numeri divisi per 12 possono dare come resto 0 oppure 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

Si formano in questo modo degli insiemi i cui elementi sono i numeri che divisi per 12 danno lo stesso resto. Tali insiemi si indicano con classi resto modulo 12 e si indicano con $[0]$; $[1]$; $[2]$;

L'insieme delle classi resto modulo 12 si indica con $\mathbb{Z}_{12}$

Operazioni nelle classi resto

Nelle classi resto vengono definite le operazioni di addizione e moltiplicazione. Aiutiamoci con delle tabelle per capire il funzionamento di queste operazioni

$$\mathbb{Z}_3$$

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

.	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

$$\mathbb{Z}_4$$

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

.	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Osserva le particolarità delle tabelle moltiplicative. Lo zero si ottiene in modi diversi. Cosa succede?

Costruisci tabelle analoghe in $\mathbb{Z}_5$

Ora avendo capito il procedimento calcola senza tabella i risultati delle seguenti operazioni in $\mathbb{Z}_{21}$ (a noi interessa perché abbiamo associato a questa classe di resto l'alfabeto italiano per la codifica e decodifica dei messaggi):

$$[19] + [7] =$$

$$[4] * [7] =$$

ARITMETICA MODULARE IN Z_{12}

Costruire la tabella della somma

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
[0]												
[1]												
[2]												
[3]												
[4]												
[5]												
[6]												
[7]												
[8]												
[9]												
[10]												
[11]												

Costruire la tabella del prodotto

*	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
[0]												
[1]												
[2]												
[3]												
[4]												
[5]												
[6]												
[7]												
[8]												
[9]												
[10]												
[11]												

Riepilogo operazioni

Operazioni

- def. di **somma** in Z_n : $\overline{a + b} = \overline{a} + \overline{b}$
- def. di **prodotto** in Z_n : $\overline{a \cdot b} = \overline{a} \cdot \overline{b}$
- def. di **potenza** in Z_n : $\overline{a^n} = \overline{a}^n$
(discende dal prodotto)

Esercizio1: Determinare il resto della divisione per 10 del numero 2345^{2008} , qual è l'ultima cifra di questo numero?

Esercizio2: Per ciascuno dei seguenti numeri individuare il minimo intero positivo modulo 12 a cui è congruente: 19, 149, -11, -128

Esercizio3: Se adesso sono le 14 che ora del giorno o della notte sarà tra 1000 ore?

Esercizio4: Se lo scorso anno Natale era Martedì in che giorno cadrà Natale quest'anno e nel 2020?