

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 adesso la tabella moltiplicativa di \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):

$$[19]+[7], \quad [4] \cdot [7]$$

CIFRARIO AFFINE

Adesso con le operazioni che abbiamo imparato riprendiamo il nostro alfabeto e ricordiamoci che ad ogni lettera avevamo associato un numero naturale da 0 a 20.

Applichiamo al nostro alfabeto, in \mathbb{Z}_{21} quindi, delle operazioni e precisamente $5n+4$ e $3n+4$ e osserviamo le due tabelle

Posizione e lettera	Nuova posizione della lettera dopo aver eseguito l'operazione $5n+4$	Posizione e lettera	Nuova posizione della lettera dopo aver eseguito l'operazione $5n+4$	Posizione e lettera	Nuova posizione della lettera dopo aver eseguito l'operazione $5n+4$
0 A	4	7 H	18	14 Q	11
1 B	9	8 I	2	15 R	16
2 C	14	9 L	7	16 S	0
3 D	19	10 M	12	17 T	5
4 E	3	11 N	17	18 U	10
5 F	8	12 O	1	19 V	15
6 G	13	13 P	6	20 Z	20

Posizione e lettera	Nuova posizione della lettera dopo aver eseguito l'operazione $3n+4$	Posizione e lettera	Nuova posizione della lettera dopo aver eseguito l'operazione $3n+4$	Posizione e lettera	Nuova posizione della lettera dopo aver eseguito l'operazione $3n+4$
0 A	4	7 H	4	14 Q	4
1 B	7	8 I	7	15 R	7
2 C	10	9 L	10	16 S	10
3 D	13	10 M	13	17 T	13
4 E	16	11 N	16	18 U	16
5 F	19	12 O	19	19 V	19
6 G	1	13 P	1	20 Z	1

La seconda tabella presenta due gravissimi problemi. Quali? Perché?

Certamente non possiamo andare per tentativi, quindi dobbiamo trovare un modo per eliminare questi problemi.

Sapresti individuare perché la moltiplicazione per 3 ha dato problemi, ma non quella per 5?