Crittografia e aritmetica modulare - 1 classe 4E

Nome: _____

Aritmetica modulo 7

Considera gli interi dell'insieme $\mathbb{Z}_7$ e l'operazione $\otimes$ così definita:

$$a \otimes b \qquad \text{è il resto della divisione di } ab \text{ per } 7$$

in altre parole, per calcolare $a \otimes b$ dobbiamo eseguire la normale moltiplicazione, dividere per 7 e prendere il resto. Per esempio $3 \otimes 4 = 5$ perché $3 \cdot 4 = 12$ che, diviso per 7, ha come resto 5 (niente di strano, è la *normale* moltiplicazione in modulo 7, solo che la indichiamo col simbolo $\otimes$)

1. Completa la tabella della moltiplicazione $\otimes$ in $\mathbb{Z}_7$:

$\otimes$	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						

Tabella 1: moltiplicazione in $\mathbb{Z}_7$

2. La tabella 1 rivela molte proprietà della moltiplicazione in $\mathbb{Z}_7$. Per rispondere alle seguenti domande osservala attentamente:

   (a) Se $a, b \in \mathbb{Z}_7$ è possibile che $a \times b$ sia un multiplo di 7? (Attenzione ai simboli: qui si parla della normale moltiplicazione!) _____
   Spiega:

   _____

   _____

   (b) L'operazione $\otimes$ è chiusa[1] in $\mathbb{Z}_7$?_____

   (c) Se $a, b \in \mathbb{Z}_7$ è sempre vero che $a \otimes b = b \otimes a$?____

[1] Un'operazione si dice *chiusa* in un insieme A se il suo risultato è sempre contenuto in A. Per esempio, la normale addizione non è chiusa nell'insieme $A = \{1, 2, 3\}$ perché 2+2=4 che non è nell'insieme A

(d) Se $a, b, c \in \mathbb{Z}_7$ e se $a \neq b$ è possibile che risulti $a \otimes c = b \otimes c$? ____ . Spiega:

(e) Se $c \in \mathbb{Z}_7$, è sempre possibile trovare un altro elemento $z \in \mathbb{Z}_7$ tale che $c \otimes z = z \otimes c = 1$? _____ [2]. Spiega il perché:

Aritmetica in $\mathbb{Z}_6$ - Non tutti gli insiemi $\mathbb{Z}_n$ hanno le stesse proprietà di $\mathbb{Z}_7$. Consideriamo ad esempio $\mathbb{Z}_6$, con l'usuale moltiplicazione $\otimes$ in modulo 6.

3. Completa la tabella della moltiplicazione in $\mathbb{Z}_6$

$\otimes$	1	2	3	4	5
1					
2					
3					
4					
5					

Tabella 2: moltiplicazione in $\mathbb{Z}_6$

4. Rispondi alle seguenti domande, osservando attentamente la tabella 3

(a) Se $a, b \in \mathbb{Z}_6$ è possibile che $a \times b$ sia un multiplo di 6? _____ . Spiega:

(b) L'operazione $\otimes$ è chiusa nell'insieme degli interi **non nulli** di $\mathbb{Z}_6$? _____ .

(c) Se $a, b, c \in \mathbb{Z}_6$ e se $a \neq b$ è possibile che $c \otimes a = c \otimes b$? _____ . Spiega o mostra un esempio:

[2] In pratica, ti sto chiedendo se ogni elemento $c \in \mathbb{Z}_7$ ha un suo inverso c^{-1}

(d) Se $c \in \mathbb{Z}_6$, è sempre possibile trovare un altro elemento $z \in \mathbb{Z}_6$ tale che $c \otimes z = z \otimes c = 1$?_____[3]. Spiega il perché:

5. Identifica quali differenze tra i numeri 6 e 7 spiegano le diverse proprietà dell'operazione $\otimes$ negli inziemi $\mathbb{Z}_6$ e $\mathbb{Z}_7$

Crittografare in $\mathbb{Z}_{31}$

L'aritmetica modulare può essere usata per la codifica e decodifica dei messaggi. Nelle pagine seguenti imparerai a codificare un messaggio utilizzando l'aritmetica modulare in $\mathbb{Z}_{31}$. Dato che 31 è un numero primo, ogni elemento non nullo in $\mathbb{Z}_{31}$ ha un suo inverso, esattamente come accade in $\mathbb{Z}_7$; per esempio, l'inverso di 2 è 16, poiché $2 \times 16 = 32 = 31 + 1$ e quindi $2 \otimes 16 = 1$

6. Usando la tabella moltiplicativa in $\mathbb{Z}_{31}$, completa la tabella degli inversi in $\mathbb{Z}_{31}$:

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
x^{-1}															
x	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
x^{-1}															

Tabella 3: inversi in $\mathbb{Z}_{31}$

Una semplice tecnica crittografica si basa sulla sostituzione di lettere con numeri; poiché le lettere dell'alfabeto sono 26, ci servono almeno 26 numeri, più altri per rappresentare i segni di punteggiatura; per questo ci mettiamo nell'insieme $\mathbb{Z}_{31}$ (come vedrai, è anche necessario che il modulo sia un numero primo).

La tabella seguente propone un possibile schema di sostituzione:

[3] In pratica, ti sto chiedendo se ogni elemento $c \in \mathbb{Z}_6$ ha un suo inverso c^{-1}

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P	Q	R	S	T	U	V	W	X	Y	Z	␣	.	,	’
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Tabella 4: Tabella di sostituzione

Il simbolo ␣ (al numero 27) rappresenta lo spazio che si usa per separare le parole. Ora codifichiamo il nostro primo messaggio: `HO UN SEGRETO`, aiutandoci con la tabella seguente. Per farlo segui le istruzioni:

Testo del messaggio	H	O		U	N								
Posizione	1	2	3	4	5								
Sostituzione	8	15	27	21	14								
Valori cifrati	8	30	19	22	8								
Testo codificato	H	‘	S	V	H								

i) Completa la prima riga inserendo le lettere del messaggio (spazi compresi!)

ii) Completa la seconda riga immettendo i numeri di posizione delle lettere e di eventuali spazi o segni di punteggiatura

iii) Inserisci nella terza riga i valori corrispondenti a ciascuna lettera o segno di punteggiatura, riferendoti alla tabella 4

iv) Nella quarta riga calcola il prodotto $\otimes$, in $\mathbb{Z}_{31}$ tra i corrispondenti numeri della seconda e terza riga (per esempio nella terza colonna calcolerai $3 \otimes 27 = 19$)

v) Usando nuovamente la tabella 4, scrivi nella quinta riga la lettera corrispondente al numero della quarta riga

7. Scrivi il messaggio codificato: _____

8. Codifica il messaggio `LA MATEMATICA E’ UTILE` usando la tabella di codifica

Testo del messaggio																						
Posizione	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Sostituzione																						
Valori cifrati																						
Testo codificato																						

9. Codifica il tuo nome

_____