



Tavola n. 5.1 Le potenze in \mathbb{Z}_7

Ricorda la tavola del prodotto modulo 7 e considera la funzione

$$f_m: \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$$

tale che $f_m(x) = x^m$.
Vogliamo scoprire per quale valore di m la funzione f_m è una funzione di cifratura.

\times	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

1. Completa la tabella dei valori corrispondenti delle potenze di x :

	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}
0	0									
1	1									
2	2									
3	3									
4	4									
5	5									
6	6									

- L'elevamento al quadrato è una cifratura? E se uso un esponente pari?
- I valori di m per i quali la funzione f_m è una funzione di cifratura sono:
- Ci sono due esponenti diversi m e k per i quali le funzioni f_m e f_k coincidono? Se sì, quali?

d) Saresti in grado di completare la tabella seguente senza fare conti?

	x^{11}	x^{12}	x^{13}	x^{14}	x^{15}
0					
1	1				
2	4				
3	5				
4	2				
5	3				
6	6				

Dopo quanti passi le funzioni si ripetono?