



Tavola n. 4.6 Le potenze in \mathbb{Z}_5

Ricorda la tavola del prodotto modulo 5:

\times	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Consideriamo la funzione $f_m: \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ tale che $f_m: x \mapsto x^m$

Vogliamo scoprire per quale valore di m la funzione f_m è una funzione di cifratura.

Completa la tabella dei valori corrispondenti delle potenze di x .

Per calcolare velocemente le potenze di un elemento, ricorda che

$$x^m x^n = x^{m+n}$$

$$(x^m)^n = x^{m \cdot n}$$

	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									

- 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 due esponenti diversi m e k per i quali le funzioni f_m e f_k coincidono? Se sì, quali?
- Saresti in grado di completare la tabella seguente senza fare conti?

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

Dopo quanti passi le funzioni si ripetono?