Tavola - Il Piccolo Teorema di Fermat

$$a^{p-1} \equiv 1 \mod p \qquad [MCD(a, p) = 1]$$

	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	5	3	3	5	9	4	1
x^3	1	8	5	9	4	7	2	6	3	10
x^4	1	5	4	3	9	9	3	4	5	1
x^5	1	10	1	1	1	10	10	10	1	10
x^6	1	9	3	4	5	5	4	3	9	1
x^7	1	7	9	5	3	8	6	2	4	10
x^8										
x^9										
x^{10}										
x^{11}										

Completa la tabella accanto lavorando Modulo 11 e rispondi alle seguenti domande:

1. Per quale esponente k si ottiene sempre $a^k=1$? .....
2. Elevando a quale esponente n si ottiene $a^n=a$?.....

3. Quali degli esponenti presenti possono essere utilizzati per cifrare?.....

4. Le potenze si ripetono in modo periodico. Utilizzando le potenze già calcolate, sapresti completare le seguenti uguaglianze inserendo altri esponenti?

   $3^{17} = 3^{\cdots} = ...$ $\qquad 5^{24} = 5^{\cdots} = ...$ $\qquad 8^{99} = 8^{\cdots} = ...$

5. Completa le seguenti uguaglianze:

   $\left(3^7\right)^{\cdots} \equiv 3$ $\qquad \left(5^3\right)^{\cdots} \equiv 5$ $\qquad \left(8^9\right)^{\cdots} \equiv 8$

Tavola – Cifratura e decifratura con il Piccolo di Fermat

Cifratura di un messaggio:

Utilizzando la seguente tabella di corrispondenza alfabeto-numeri cifra il messaggio: "stai qui"

A	B	I	O	Q	S	T	U	V
2	3	4	5	6	7	8	9	10

Funzione di cifratura: $f : m \to m' = m^3 \,(\mathrm{mod}\, 11)$

S	T	A	I		Q	U	I

Messaggio cifrato:……..

Decifratura di un messaggio:

Sapendo che il messaggio 10 8 9 10 9 8 2 3 5 9 6 4

è stato cifrato con la funzione di cifratura $f : m \to m' = m^3 \,(\mathrm{mod}\, 11)$ stabilisci l'esponente α della funzione di decifratura $f^{-1} : m' \to m = (m')^a \,(\mathrm{mod}\, 11)$ e decifra il messaggio

α=.....

Messaggio cifrato:

10	8	9	10	9	8	2	3	5	9	6	4

Messaggio in chiaro:……