Tavola n. 5.6 Soluzioni: Lavoriamo modulo 33 = 3x11

$$x^m\, x^n = x^{m+n}$$
$$(x^m)^n = x^{m\ n}$$

Completa le tabella delle potenze, lavorando in Z_3

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$\mathbf{x^2}$	1	4	9	16	25	3	16	31	15	1	22	12	4	31	27	25	25	27	31	4	12	22	1	15	31	16	3	25	16	9	4	1
$\mathbf{x^3}$	1	8	27	31	26	18	13	17	3	10	11	12	19	5	9	4	29	24	28	14	21	22	23	30	16	20	15	7	2	6	25	-1
$\mathbf{x^4}$	1	16	15	25	31	9	25	4	27	1	22	12	16	4	3	31	31	3	4	16	12	22	1	27	4	25	9	31	25	15	16	1
$\mathbf{x^5}$	1	32	12		23			32		10	11	12										22	23									-1
$\mathbf{x^6}$	1	31	3							1	22	12										22	1									1
$\mathbf{x^7}$	1	29	9	16	14	30	28	2	15	10	11	12	7	20	27	25	8	6	13	26	21	22	23	18	31	5	3	19	17	24	4	32

Controlla che l'applicazione $x \mapsto x^7$ è una applicazione di cifratura (cioè è una applicazione biettiva)

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$\mathbf{y=x^7}$	1	29	9	16	14	30	28	2	15	10	11	12	7	20	27	25	8	6	13	26	21	22	23	18	31	5	3	19	17	24	4	32

Controlla che l'applicazione $y \mapsto y^3$ è l'applicazione inversa della precedente (cioè la decifratura)

y	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$\mathbf{y^3}$	1	8	27	31	26	18	13	17	3	10	11	12	19	5	9	4	29	24	28	14	21	22	23	30	16	20	15	7	2	6	25	-1

Osserva che : $(x^7)^3 = x^{7x3} = x^{21}$ e che (3-1) x (11-1) = 2 x 10 = 20. Il teorema di Eulero assicura che $x^{20} = 1$, e dunque

$$x^{21} = x^{20+1} = x^{20}\ x = x$$