



Tavola n. 5.6: Lavoriamo modulo 33 = 3x11

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

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

Completa le tabella delle potenze, lavorando in \mathbb{Z}_{33}

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
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
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
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
x^5	1																															-1
x^6	1																															1
x^7																																

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
$y=x^7$	1																															

Ricorda il corollario del teorema di Eulero, che afferma che se $n = pq$ è prodotto di due numeri primi distinti, allora

$$a^{(p-1)(q-1)+1} = a \pmod{n}.$$

Determina l'esponente t tale che l'applicazione $y \mapsto y^t$ sia l'applicazione inversa della precedente (cioè la decifratura) : $t = \dots\dots\dots$