

Si denoti \mathbf{Z}_n l'anello delle classi di congruenza modulo n e \mathbf{Z}_n^* l'insieme degli elementi di \mathbf{Z}_n che hanno un inverso.

1. Sia $n \in \mathbf{N}$. L'ordine $\text{ord}_n(x)$ di $x \in \mathbf{Z}_n^*$ è il più piccolo $r > 0$ tale che $x^r \equiv 1 \pmod{n}$.
 - (a) Sia $n = 7$. Calcolare $\text{ord}_n(x)$ per ogni $x \in \mathbf{Z}_n^*$.
 - (b) Sia n primo. Dimostrare che $\text{ord}_n(x)$ divide $n - 1$ per ogni $x \in \mathbf{Z}_n^*$.
 - (c) Sia $n \in \mathbf{N}$. Calcolare l'ordine di $-1 \pmod{n}$.
2. (a) Sia $p > 2$ un primo. Dimostrare che $\{x \in \mathbf{Z}_p : x^2 = 1\} = \{\pm 1\}$.
 - (b) Determinare tutti gli $x \in \mathbf{Z}_{15}^*$ per cui $x^2 = 1$. Stessa domanda per \mathbf{Z}_{21}^* .
 - (c) Sia n prodotto di due primi dispari. Quanti sono gli elementi $x \in \mathbf{Z}_n^*$ con $x^2 = 1$?
 - (d) Determinare tutti gli $x \in \mathbf{Z}_9^*$ per cui $x^2 = 1$. Stessa domanda per \mathbf{Z}_{25}^* .
 - (e) Sia n quadrato di un numero primo $p > 2$. Quanti sono gli elementi $x \in \mathbf{Z}_n^*$ con $x^2 = 1$?
3. La funzione φ di Eulero è definita da $\varphi(n) = \#\mathbf{Z}_n^*$ (per $n \in \mathbf{N}$).
 - (a) Dimostrare: $\varphi(n) = \#\{a \in \mathbf{N} : 0 \leq a < n \text{ e } \text{mcd}(a, n) = 1\}$.
 - (b) Calcolare $\varphi(n)$ per ogni $n \leq 10$.
 - (c) Dimostrare che $\varphi(n) = n - 1$ quando n è primo.
 - (d) Sia $n = pq$ per due primi p e q . Dimostrare che $\varphi(n) = (p - 1)(q - 1)$.
 - (e) Sia p un primo. Calcolare $\varphi(p^2)$. Calcolare $\varphi(p^k)$ per ogni $k \geq 1$.
4. Un numero di Carmichael è un numero naturale che non è primo, ma per cui $x^{n-1} \equiv 1 \pmod{n}$ per ogni $x \in \mathbf{Z}_n^*$.
 - (a) Dimostrare che $561 = 3 \cdot 17 \cdot 31$ è un numero di Carmichael.
 - (b) Dimostrare che $8911 = 7 \cdot 19 \cdot 67$ è un numero di Carmichael.
 - (c) Dimostrare che un numero di Carmichael ha almeno tre fattori primi (Sugg. usare il fatto che per ogni primo p esiste $g \in \mathbf{Z}_p^*$ di ordine $p - 1$).
5. (mini-RSA) Sia $p = 7$ e $q = 13$ e sia $n = pq = 7 \cdot 13 = 91$ il modulo di questo sistema RSA. L'esponente pubblico è $D = 11$. Il messaggio è $m = 10$.
 - (a) Cifrare il messaggio, cioè calcolare il resto \tilde{m} della divisione di m^D per n .
 - (b) Determinare l'esponente segreto E , cioè calcolare E tale che $DE \equiv 1 \pmod{(p-1)(q-1)}$.
 - (c) Decifrare \tilde{m} , cioè controllare che il resto della divisione di \tilde{m}^E per n è uguale al messaggio originale m .
6. (mini-RSA) Sia $n = 77$ il modulo di un sistema crittografico RSA. Sia $D = 13$ l'esponente che si usa per cifrare i messaggi. Determinare un esponente $E \in \mathbf{N}$ tale che $(x^D)^E \equiv x \pmod{n}$ per il messaggio $x = 4$.
7. Per trasformare un testo in una serie di numeri, usiamo questa tabella.

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	spazio
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	00

- (a) Far vedere che il testo "PIPPO BAUDO" viene trasformato in "1409141413000201190413". Il modulo del sistema RSA usato in questo esercizio è uguale a $n = 2000000002864822776563$. L'esponente pubblico è uguale a $D = 25042003$.
- (b) Far vedere che il messaggio "1409141413000201190413" della parte (a), cifrato tramite questo sistema RSA, è uguale a 474795864046624770221.
- (c) Si intercetta il messaggio cifrato $\tilde{m} = 605233533198702885420$. Cercare di rompere questo sistema e di decifrare e leggere il messaggio. (Suggerimento: trovare la fattorizzazione $n = pq$ e calcolare l'esponente segreto, cioè determinare E tale che $DE \equiv 1 \pmod{(p-1)(q-1)}$. Il messaggio originale è allora uguale a $\tilde{m}^E \pmod{n}$.)