1. Sia $\mathbf{Z}[i]$ il sottoinsieme di $\mathbf{C}$ dato da $\{a+bi \in \mathbf{C} : a, b \in \mathbf{Z}\}$.
   (a) Dimostrare che si tratta di un anello commutativo.
   (b) Dimostrare che $a+bi \in \mathbf{Z}[i]$ è invertibile, se e solo se $a^2+b^2=1$.
   (c) Enumerare gli elementi del gruppo $\mathbf{Z}[i]^*$ degli elementi invertibili.

2. (*Anello di Boole*) Sia X un isieme e sia $P(X)$ l'insieme dei sottoinsiemi di X. Definiamo per $A, B \in P(X)$

$$A + B = A \Delta B \ (= \ A \cup B - A \cap B),$$
$$A \cdot B = A \cap B.$$

   Dimostrare che con quest'addizione e moltiplicazione $P(X)$ diventa un anello commutativo.

3. Un *numero di Carmichael* è un numero naturale che non è primo, ma per cui si ha che $x^{n-1} \equiv 1 \pmod{n}$ per ogni $x \in \mathbf{Z}_n^*$.
   (a) Dimostrare che $561 = 3 \cdot 17 \cdot 11$ è un numero di Carmichael.
   (b) Dimostrare che $1105 = 5 \cdot 13 \cdot 17$ è un numero di Carmichael.

4. Per trasformare un testo in una serie di cifre, usiamo questa tabella.

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

   Lo spazio viene trasformato in "00".
   (a) Verificare che il testo "MAMMA MIA" viene trasformato in "11011110100110901".

   Il modulo del criptosistema RSA usato in questo esercizio è uguale a

$$n = 518253916955473343412775938632606450609758843063044948674743.$$

   L'esponente pubblico è uguale a $E = 65537$.
   (b) Far vedere che il messaggio "11011110100110901" della parte (a), cifrato tramite questo sistema RSA, diventa

$$454523371038768686089969735874772812678752746688571724998808.$$

   (c) Supponiamo di intercettare il messaggio cifrato

$$\tilde{m} = 127948630281966754520946338302735813129055214929923845505060.$$

   Cercare di rompere questo sistema e di decifrare e leggere il messaggio. (Suggerimento: in qualche modo trovare la fattorizzazione $n = pq$ e calcolare l'esponente segreto, cioè determinare D tale che $DE \equiv 1 \pmod{(p-1)(q-1)}$. Il messaggio originale è allora uguale a $\tilde{m}^D \pmod{n}$.)