1. (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 $D \in \mathbf{N}$ 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.

2. (a) Sia $n = 77$ il modulo di un sistema 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 ogni messaggio $x \in \mathbf{Z}_{77}^*$.
   (b) Sia $n = 55$ il modulo di un sistema 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 ogni messaggio $x \in \mathbf{Z}_{55}^*$.

3. (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 $x^2 = 1$?

4. (a) Sia $p > 2$ un primo. Quanto sono gli elementi $x \in \mathbf{Z}_p^*$ tali che $x^2 = \bar{4}$?
   (b) Determinare tutti gli $x \in \mathbf{Z}_{15}^*$ per cui $x^2 = \bar{4}$. Stessa domanda per $\mathbf{Z}_{21}^*$.
   (c) Sia n prodotto di due primi dispari. Quanti sono gli elementi $x \in \mathbf{Z}_n^*$ con $x^2 = \bar{4}$?
   (d) Determinare tutti gli $x \in \mathbf{Z}_9^*$ per cui $x^2 = \bar{4}$. 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 $x^2 = \bar{4}$?

5. Si consideri il seguente modo (molto primitivo) di criptare i messaggi: si presuppone che l'alfabeto abbia 25 lettere. Ad ogni lettera (a,b,c...) si associa il corrispondente numero progressivo (1,2,3..). Per criptare una lettera corrispondente al numero x, si usa la funzione $f : \mathbf{Z}_{25} \to \mathbf{Z}_{25}$, $f(\overline{x}) = \overline{7x + 18}$. Che funzione deve usare il ricevente per decodificare il messaggio?
   Si può usare $f(\overline{x}) = \overline{10x + 21}$ come funzione di codifica?

6. Sia $L, \wedge, \vee$ un reticolo e si consideri l'associata relazione su L, denotata " $\leq$ ": dati $a, b \in L$, $a \leq b$ se e solo se $a \vee b = b$.
   (a) Dimostrare che $a \leq b$ se e solo se $a \wedge b = a$;
   (b) Dimostrare che la relazione " $\leq$ " è una relazione d'ordine.
   (c) Dimostrare che , secondo la relazione d'ordine " $\leq$ ", $inf(a, b) = a \wedge b$ e $sup(a, b) = a \vee b$, per ogni $a, b \in L$.

7. Sia $L, \leq$ un insieme parzialmente ordinato tale che, per ogni $a, b \in L$, $sup(a, b)$ e $inf(a, b)$ esistono. Si definiscano le seguenti operazioni su L: $a \wedge b = inf(a, b)$ e $a \vee b = sup(a, b)$.
   Dimostrare che $L, \wedge, \vee$ é un reticolo (cioè che le due operazioni sono commutative, associative, e verificano la legge di assorbimento).

8 . Stabilire quali dei seguenti insiemi parzialmente ordinati ($A \leq B$ se e solo se $A \subseteq B$) sono reticoli:
   (a) $\{A \in \mathcal{P}(\{1, 2, 3, 4, 5\}) : |A| \text{ dispari }\}$;
   (b) $\{A \in \mathcal{P}(\{1, 2, 3, 4, 5\}) : |A| \geq 2\}$;
   (c) $\{A \in \mathcal{P}(\{1, 2, 3, 4, 5\}) : A \supset \{1, 3\}\}$;
   (d) $\{A \in \mathcal{P}(\{1, 2, 3\}) : |A| \leq 1 \text{ oppure } |A| = 3\}$.

9 . Per le coppie $(n, m) = (6, 15)$, $(12, 18)$ e $(30, 105)$,
   (a) Stabilire se i reticoli $\mathbf{D}_n$ e $\mathbf{D}_m$ sono isomorfi.
   (b) In caso affermativo determinare tutti gli isomorfismi di reticolo $f : \mathbf{D}_n \to \mathbf{D}_m$.
   (c) Stabilire se i reticoli $\mathcal{P}(\{1, 2, 3\})$ e $\mathbf{D}_{24}$ sono isomorfi.
   (d) Stabilire se uno dei reticoli del punto (c) è isomorfo a $\mathbf{D}_{30}$.

10 . Sia $n \in \mathbf{N}$. Dinostrare che il reticolo $\mathbf{D}_n$ è complementato se e solo se n è prodotto di primi distinti (suggerimento: se la fattorizzazione in primi di n è $n = p_1^{r_1} \cdots p_k{}^{r_k}$, considerare, per esempio $a = p_1$ e vedere sotto quali condizioni esiste un complemento di A).

11 . Si consideri il seguente insieme parzialmente ordinato $L = \{A \in \mathcal{P}(\{1, 2, 3, 4\}) : |A| \leq 1 \text{ oppure } |A| = 4\}$ ($A \leq B$ se e solo se $A \subseteq B$). Verificare che è un reticolo.
   (a) Dimostrare che L è limitato.

(b) Stabilire se ci sono elementi il cui complemento non è unico e in tal caso, indicare quali elementi e perchè.
(c) Stabilire se L è un reticolo distributivo (in caso negativo, mostrare esplictamente tre elementi che non verificano una delle due ditributività).

10. Stabilire se i seguenti insiemi parzialmente ordinati sono reticoli, reticoli distributivi, reticoli con complemento, reticoli con complemento unico. In caso negativo, dimostrare che la proprietà in questione non è verificata esibendo esplicitamente un controesempio.
(a) $\{1, 2, 3, 4, 9, 12, 18, 36\}$, ordinato tramite la divisbilità;
(b) $\mathbf{D}_{12}$,
(c) $\mathcal{P}(\{a, b, c\})$,
(d) $\mathbf{D}_{30}$,
(e) $\{1, 6, 10, 15, 30, 60, 90, 180\}$, ordinato tramite la divisibilità.
(f) $\{1, 2, 3, 15, 30, 60, 90, 180\}$, ordinato tramite la divisibilità.