Esercizio 1. Risolvere i seguenti sistemi di equazioni congruenziali:

(a)
$$\begin{cases} x \equiv 4 & \mod 8 \\ x \equiv 3 & \mod 5 \\ x \equiv 4 & \mod 9 \end{cases}$$

(b)
$$\begin{cases} 5x \equiv 4 & \mod 8 \\ 3x \equiv 3 & \mod 5 \\ 2x \equiv 4 & \mod 9 \end{cases}$$

Esercizio 2. Calcolare il resto nella divisione per 10 di 3^{51}.

Esercizio 3. Calcolare il resto nella divisione per 5 di 22^8.

Esercizio 4. Si consideri il sistema crittografico RSA relativo al modulo $n := 143 = 11 \cdot 13$ e all'esponente $e := 53$.

(a) Cifrare il messaggio 24, cioè calcolare la classe resto modulo 143 di 24^{53}.

(b) Determinare un esponente d che consenta di decifrare il messaggio, cioè tale che $(24^{53})^d \equiv 24 \mod 143$.

Esercizio 5. Sia $D_n = \{\text{divisori di } n\}$ con l'ordinamento δ dato da $a \,\delta\, b$ se a divide b. Disegnare i diagrammi di Hasse di D_{27}, D_{15}, D_{42}.

Esercizio 6. Disegnare il diagramma di Hasse dell'insieme $\mathcal{P}(\{a, b, c, d\})$ ordinato per inclusione.

Esercizio 7. Dimostrare che gli insiemi parzialmente ordinati dei due esercizi precedenti sono reticoli.

Esercizio 8. Si consideri $D = D_6 \times D_{10}$ ordinati tramite l'*ordinamento lessicografico*. Trovare (se esistono) inf e sup di $\{(2,2),(2,5)\}$ e $\{(3,1),(2,5)\}$. Inoltre, D è un reticolo?