COGNOME ..... *NOME* .....

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare ed essenziali.*
NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 6 punti.

1. *In un'algebra di Boole* $(\mathcal{A}, \cdot, +, ')$ *si consideri l'espressione* $E(x,y,z) = xy'z' + x'z' + x'yz' + x'y$. *Usando il metodo del consenso, determinare tutti gli implicanti primi di* E.

Usando l'assorbimento, $(1+y) = 1$,

$$E(x,y,z) = xy'z' + x'z' + x'yz' + x'y = xy'z' + x'z'(1+y) + x'y = xy'z' + x'z' + x'y.$$

Il consenso fra $xy'z'$ e $x'z'$ è dato da $Q = y'(z')^2 = y'z'$, da cui

$$xy'z' + x'z' + x'y = xy'z' + x'z' + x'y + y'z' = (x+1)y'z' + x'z' + x'y = y'z' + x'z' + x'y,$$

usando l'assorbimento $(1+x) = 1$. L'unico consenso non nullo è il consenso fra $y'z'$ e $x'y$, dato da $Q = z'x'$; poiché appartiene già ad E, si può trascurare. Di conseguenza

$$y'z' + x'z' + x'y$$

è la somma di tutti gli implicanti primi di E.

2. *Si definisca:* $w_0 = 2$, $w_1 = 3$ *e, per ogni* $n \geq 2$, $w_n = w_{n-1} + w_{n-2}$. *Dimostrare che* $w_0^2 + w_1^2 + \cdots + w_n^2 = w_n w_{n+1} - 2$ *per ogni* $n \geq 1$.

Si dimostra l'asserzione richiesta per induzione.
Per $n = 1$ è vera: $w_0^2 + w_1^2 = 13$ e $w_1 w_2 - 2 = 3 \cdot 5 \cdot 2 = 13$.
Passo induttivo: assumiamo per ipotesi che $w_1^2 + \ldots + w_n^2 = w_n w_{n+1} - 2$ e dimostriamo che

$$w_1^2 + \ldots + w_n^2 + w_{n+1}^2 = w_{n+1} w_{n+2} - 2.$$

Per l'ipotesi induttiva abbiamo

$$w_1^2 + \ldots + w_n^2 + w_{n+1}^2 = w_n w_{n+1} - 2 + w_{n+1}^2 = w_{n+1}(w_n + w_{n+1}) - 2. \qquad (*)$$

Poiché per definizione vale $w_{n+2} = w_n + w_{n+1}$, l'espressione (*) è uguale a $w_{n+1} w_{n+2} - 2$, come richiesto.

3. *Sia* A *un insieme. Si definisca la seguente relazione su* $\mathcal{P}(A)$*:* $U \, R \, W$ *se e solo se* $|U| = |W|$ *oppure* $|U| = |W^c|$ *(si ricorda che* $|U|$ *denota la cardinalità di* U *e* W^c *denota l'insieme* $\{a \in A \mid a \notin W\}$*).*
   (a) Stabilire se R *è una relazione di equivalenza.*
   (b) In caso affermativo, stabilire quante sono le classi di equivalenza di $\mathcal{P}(\{1,2,3,4,5,6,7,8,9,10\})$ *rispetto alla relazione* R *(motivare la risposta).*

(a) R è riflessiva, ossia $U \, R \, U$, $\forall U \in \mathcal{P}(A)$, in quanto $|U| = |U|$, $\forall U \in \mathcal{P}(A)$.
R è simmetrica, ossia se $U \, R \, W$ allora $W \, R \, U$: infatti se $|U| = |W|$ anche $|W| = |U|$; similmente, se $|U| = |W^c|$, allora $|W| = |U^c|$.
R è transitiva, ossia se $U \, R \, W$ e $W \, R \, T$, allora $U \, R \, T$: infatti si ha che

$$\begin{aligned}
|U| = |W|,\ |W| = |T| \quad &\Rightarrow \quad |U| = |T| \\
|U| = |W^c|,\ |W| = |T| \quad &\Rightarrow \quad |U| = |W^c| \text{ e } |W^c| = |T^c| \quad \Rightarrow \quad |U| = |T^c| \\
|U| = |W|,\ |W| = |T^c| \quad &\Rightarrow \quad |U| = |T^c| \\
|U| = |W^c|,\ |W| = |T^c| \quad &\Rightarrow \quad |U| = |W^c| \text{ e } |W^c| = |T| \quad \Rightarrow \quad |U| = |T|.
\end{aligned}$$

(b) Poiché dato $U \in \mathcal{P}(A)$, vale $|U^c| = 10 - |U|$, due sottoinsiemi $U, W \in \mathcal{P}(A)$ sono in relazione se e solo se $|U| = |W|$ oppure $|U| = 10 - |W|$. Ne segue che le classi di equivalenza sono 6 e sono costituite rispettivamente dai sottoinsiemi di cardinalità $0, 1, 2, 3, 4, 5$.

4. *Si consideri il reticolo* $(\mathbf{D_{405}}, \mathrm{mcd}, \mathrm{mcm})$*, dove* $\mathbf{D_{405}} = \{n \in \mathbb{N} \mid n \text{ divide } 405\}$.
   (a) *Determinare se* $\mathbf{D_{405}}$ *è un reticolo complementato (verificare che ogni elemento ammette complemento oppure esibire almeno un elemento che non ammette complemento).*
   (b) *Enunciare la proposizione "Il reticolo* $\mathbf{D_{405}}$ *è distributivo" usando quantificatori e connettivi logici.*
   (c) *Verificare se l'enunciato formulato al punto (b) è vero o falso sulla terna* $x = 9$*,* $y = 5$*,* $z = 45$*.*

(a) Il reticolo $\mathbf{D_{405}}$ non è complementato:
l'elemento 15 non ha complemento in $\mathbf{D_{405}}$: infatti se $m \in \mathbf{D_{405}}$ ha la proprietà che $\mathrm{mcd}(15, m) = 1$, allora necessariamente $m = 1$. D'altra parte $\mathrm{mcm}(15, 1) = 15 \neq 405$ ed $m = 1$ non è un complemento di 15.
(b)

$$\forall x, y, z \in \mathbf{D_{405}} \quad \mathrm{mcd}(x, \mathrm{mcm}(y, z)) = \mathrm{mcm}(\mathrm{mcd}(x, y), \mathrm{mcd}(x, z));$$

$$\forall x, y, z \in \mathbf{D_{405}} \quad \mathrm{mcm}(x, \mathrm{mcd}(y, z)) = \mathrm{mcd}(\mathrm{mcm}(x, y), \mathrm{mcm}(x, z)).$$

(c)

$$\mathrm{mcd}(9, \mathrm{mcm}(5, 45)) = \mathrm{mcm}(\mathrm{mcd}(9, 5), \mathrm{mcd}(9, 45)), \quad \mathrm{mcd}(9, 45) = 9 = \mathrm{mcm}(1, 9);$$

$$\mathrm{mcm}(9, \mathrm{mcd}(5, 45)) = \mathrm{mcd}(\mathrm{mcm}(9, 5), \mathrm{mcm}(9, 45)), \quad \mathrm{mcm}(9, 5) = 45 = \mathrm{mcd}(45, 45).$$

5. *Si consideri il sistema RSA di modulo* $n = 143 = 11 \cdot 13$ *ed esponente pubblico* $E = 37$*.*
   (a) *Cifrare il messaggio* $m = 56$*. Calcolare cioè il resto, che si denoterà* $\widetilde{m}$*, della divisione per* 143 *del numero* 56^{37}*.*
   (b) *Decifrare il messaggio* $\widetilde{m}$*. Calcolare cioè l'esponente segreto* D *tale che* $\widetilde{m}^D \equiv m \mod 143$*.*

(a) Si ha che $56 \equiv 1 \bmod 11$, e quindi $56^{37} \equiv 1 \bmod 11$. Inoltre, $37 \equiv 1 \bmod 12$, da cui $56^{37} \equiv 4^{37} \equiv 4^1 \equiv 4 \bmod 13$. Ne segue che il resto della divisione per 143 di 56^{37} è il numero intero x, con $0 \leq x \leq 142$, che soddisfa il sistema di congruenze

$$\begin{cases} x \equiv 1 \bmod 11 \\ x \equiv 4 \bmod 13. \end{cases}$$

Tale numero risulta $x = 56$, per cui in questo caso particolare $m = \widetilde{m} = 56$.
(b) In questo caso particolare, per il fatto che $m = \widetilde{m}$, è evidente che $D = 1$ soddisfa le condizioni richieste. In generale, l'esponente segreto D è l'inverso di 37 modulo $(11 - 1)(13 - 11) = 10 \cdot 12 = 120$ e si calcola risolvendo la congruenza

$$37x \equiv 1 \bmod 120.$$

Con l'algoritmo euclideo si trova

$$\mathrm{mcd}(37, 120) = 1, \qquad 37 \cdot 13 + (-4) \cdot 120 = 1,$$

per cui l'esponente segreto risulta $D = 13$.