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 7,5 punti.

1. *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 $D = 13$.

2. *Considerare l'enunciato*
   $P(x)$: $\forall x \in]-\infty, -1/2[\quad (x^2 + 2x + 1 > 0) \wedge (x < 0) \bigvee (x^2 + 2x + 1 < 0) \wedge (x > 0)$.
   (a) Determinare se $P(x)$ *è vero.*
   (b) Determinare $\neg P(x)$, *ossia la negazione di* $P(x)$ *(non ci devono essere negazioni davanti ad un quantificatore o ad un connettivo logico).*

(a) L'enunciato $P(x)$ è falso:

$$\forall x \in]-\infty, -1/2[\quad (x^2 + 2x + 1 < 0) \wedge (x > 0)$$

è falso perché $\forall x \in]-\infty, -1/2[\quad x > 0$ è falso; inoltre scrivendo $x^2 + 2x + 1 = (x+1)^2$ vediamo che la disequazione $x^2 + 2x + 1 > 0$ è soddisfatta da tutti i numeri reali $x \neq -1$. Poiché $-1 \in]-\infty, -1/2[$, si ha che anche

$$\forall x \in]-\infty, -1/2[\quad (x^2 + 2x + 1 > 0) \wedge (x < 0)$$

è falso, per cui $P(x)$ è falso.
(b) $\neg P(x)$:

$$\begin{aligned}
&\neg(\forall x \in]-\infty, -1/2[\quad (x^2 + 2x + 1 > 0) \wedge (x < 0) \bigvee (x^2 + 2x + 1 < 0) \wedge (x > 0) \\
&\exists x \in]-\infty, -1/2[\quad \neg((x^2 + 2x + 1 > 0) \wedge (x < 0) \bigvee (x^2 + 2x + 1 < 0) \wedge (x > 0)) \\
&\exists x \in]-\infty, -1/2[\quad \neg((x^2 + 2x + 1 > 0) \wedge (x < 0)) \bigwedge \neg((x^2 + 2x + 1 < 0) \wedge (x > 0)) \\
&\exists x \in]-\infty, -1/2[\quad \neg(x^2 + 2x + 1 > 0) \vee \neg(x < 0) \bigwedge \neg(x^2 + 2x + 1 < 0) \vee \neg(x > 0) \\
&\exists x \in]-\infty, -1/2[\quad (x^2 + 2x + 1 \leq 0) \vee (x \geq 0) \bigwedge (x^2 + 2x + 1 \geq 0) \vee (x \leq 0).
\end{aligned}$$

3. *In un'algebra di Boole* $(\mathcal{A}, \cdot\,, +, ')$ *si consideri l'espressione* $E(x, y, z) = xy'z' + x'z' + x'yz' + x'y$.

(a) Usando il metodo del consenso, determinare tutti gli implicanti primi di E.
(b) Determinare una forma minimale di E.

(a) 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 ancora l'assorbimento $(x + 1) = 1$. 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.
(b) Per ottenere una forma minimale di E, "completiamo" gli implicanti primi trovati al punto precedente:

$$y'z' = xy'z' + x'y'z', \quad x'z' = yx'z' + y'x'z', \quad x'y = x'yz + x'yz'.$$

Poiché entrambi gli addendi di $x'z'$ sono già presenti fra gli addendi di $y'z'$ e di $x'y$, possiamo eliminare $x'z'$ ed una forma minimale di E risulta

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

In questo caso è anche unica.

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) Verificare che $\mathbf{D_{405}}$ *è un reticolo limitato.*
   (b) Determinare se $\mathbf{D_{405}}$ *è un reticolo complementato (verificare che ogni elemento ammette complemento oppure esibire almeno un elemento che non ammette complemento).*
   (c) Enunciare la proposizione "Il reticolo $\mathbf{D_{405}}$ *è distributivo" usando quantificatori e connettivi logici.*
   (d) Verificare se l'enunciato formulato al punto (c) è vero o falso sulla terna $x = 9$*,* $y = 5$*,* $z = 45$*.*

Poiché $405 = 3^4 \cdot 5$, il reticolo $\mathbf{D_{405}}$ è dato da

$$\mathbf{D_{405}} = \{1, 3, 9, 27, 81, 5, 15, 45, 135, 405\}.$$

L'ordinamento parziale sul reticolo è dato da: $m \leq n$ *se* m *divide* n.
(a) Il reticolo $\mathbf{D_{405}}$ è limitato:
il minimo è 1: infatti 1 divide tutti gli elementi di $\mathbf{D_{405}}$ e dunque $1 \leq n$, per ogni $n \in \mathbf{D_{405}}$.
il massimo è 405: infatti ogni gli elemento di $\mathbf{D_{405}}$ divide 405 e dunque $n \leq 405$, per ogni $n \in \mathbf{D_{405}}$.
(b) 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.
(c)

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

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

(d)

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

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