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 $n = 91 = 13 \cdot 7$ ed esponente pubblico $e = 7$.
   (a) Cifrare il messaggio $w = 20$. Chiamiamo il risultato w'.
   (b) Calcolare una chiave di decodifica, ovvero calcolare un esponente "segreto" d tale che $(w')^d \equiv w \pmod{91}$.

(a) Abbiamo che $w' \equiv 20^7 \pmod{91}$. Siccome si ha $20^2 = 400 \equiv 36 \pmod{91}$, vale anche $20^3 = 20 \cdot 36 = 730 \equiv -8 \pmod{91}$ e quindi $20^7 = 20(-8)^2 = 1280 \equiv 370 \equiv 6 \pmod{91}$. Abbiamo quindi che $w' \equiv 6 \pmod{91}$.
(b) Siccome $\varphi(91) = \varphi(13 \cdot 7) = 12 \cdot 6 = 72$, un qualsiasi $d \in \mathbf{N}$ che soddisfa $ed \equiv 1 \pmod{72}$ è un esponente 'segreto' valido. Calcoliamo il mcd di $e = 7$ con 72. Abbiamo che

$$\begin{aligned} 1 \cdot 72 + 0 \cdot 7 &= 72, \\ 0 \cdot 72 + 1 \cdot 7 &= 7, \\ 1 \cdot 72 - 10 \cdot 7 &= 2, \\ -3 \cdot 72 + 31 \cdot 7 + 1. \end{aligned}$$

Concludiamo che $7 \cdot 31 \equiv 1 \pmod{72}$. Un'esponente segreto è quindi dato da $d = 31$.

2. In un'algebra di Boole $(A, \cdot, +, ')$ si consideri l'espressione $E(x, y, z) = xy'z' + xx'y + x'z' + xyz' + x'y$.
   (a) Scrivere E sotto forma di somma di prodotti.
   (b) Usando il metodo del consenso, scrivere E come somma di implicanti primi.
   (c) Determinare una forma minimale di E.

(a) Sappiamo che $xx' = 0$; quindi riscriviamo E sotto forma di somma di prodotti nel modo seguente

$$E = xy'z' + x'z' + xyz' + x'y$$

(b) Sommiamo i consensi del primo e secondo, primo e terzo e terzo e quarto addendo: $E = xy'z' + x'z' + xyz' + x'y + y'z' + xz' + yz'$. Per assorbimento otteniamo $E = x'z' + x'y + y'z' + xz' + yz'$; a questo sommiamo il consenso del primo e del quarto membro e di nuovo applichiamo l'assorbimento: $E = x'y + z'$. Questa è la scrittura di E come somma di impicanti primi.
(c) Essendo la scrittura come somma di implicanti primi una forma minimale, il punto precedente risponde anche a questa domanda.

3. Sia $A = \{1, 2, 3, 4\}$ e sia $P = \{B \subset A : \#B \text{ è dispari}\}$. Sia R su P la relazione data da "B è in relazione con C quando $B \subset C$".
   (a) Dimostrare che si tratta di un ordinamento parziale.
   (b) Determinare, se esistono, elementi massimali e minimali.
   (c) Determinare, se esistono, massimi e minimi assoluti.
   (d) Determinare, se esiste, $\sup(\{1\}, \{2\})$.

(a) Ogni sottoinsieme B di A è contenuto in se stesso; se abbiamo che $B \subset C$ e anche $C \subset B$, allora $B = C$; se abbiamo $B \subset C$ e anche $C \subset D$, allora $A \subset D$. La relazione è quindi riflessiva, anti-simmetrica e transitiva. In altre parole, si tratta di un ordinamento parziale.
(b) Abbiamo che $P = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}\}$. I quattro sottoinsiemi di un elemento, non contengono altri sottoinsiemi di A e sono quindi elementi minimali nell'ordinamento parziale. Similmente i quattro sottoinsiemi di cardinalità 3 sono elementi massimali.
(c) Non c'è nessun elemento di P che contiene ogni altro elemento di P. Non esiste quindi un massimo assoluto. Similmente, non esiste nessun elemento di P contenuto in ogni altro elemento di P e non esiste un minimo assoluto.
(d) I maggioranti comuni di $\{1\}$ e $\{2\}$ sono $\{1, 2, 3\}$ e $\{1, 2, 4\}$. Non esiste quindi un maggiorante comune che è contenuto in ogni altro maggiorante. Concludiamo che $\sup(\{1\}, \{2\})$ non esiste.

4. Dimostrare per induzione che 21 divide $4^{n+1} + 5^{2n-1}$ per ogni $n \in \mathbf{N}$.

La formula vale per $n = 1$, perché abbiamo che $4^2 + 5^1 = 21$. Per dimostrare la formula per $n + 1$, scriviamo

$$\begin{aligned} 4^{n+2} + 5^{2(n+1)-1} &= 4(4^{n+1} + 5^{2n-1}) - 4 \cdot 5^{2n-1} + 5^{2(n+1)-1}, \\ &= 4(4^{n+1} + 5^{2n-1}) - 5^{2n-1}(-4 + 25), \\ &= 4(4^{n+1} + 5^{2n-1}) + 21 \cdot 5^{2n-1}. \end{aligned}$$

Siccome per ipotesi la formula vale per n, il fattore $4^{n+1} + 5^{2n-1}$ è divisibile per 21. Concludiamo che l'ultima espressione è divisibile per 21 e quindi che la formula vale per $n + 1$.