Elementi di algebra e logica. 2^o Esonero. 3 maggio 2005, 16:00–18:00.

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

   $$1 \cdot 72 + 0 \cdot 7 = 72,$$
   $$0 \cdot 72 + 1 \cdot 7 = 7,$$
   $$1 \cdot 72 - 10 \cdot 7 = 2,$$
   $$-3 \cdot 72 + 31 \cdot 7 + 1.$$

   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.

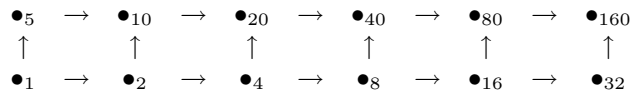
   (a) Sappiamo che $xx' = 0$; quindi riscriviamo E sotto forma di somma di prodotti nel modo seguente

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

   (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. Si consideri il reticolo ($\mathbf{D_{160}}$, **mcd**, **mcm**), dove ($\mathbf{D_{160}}$ è l'insieme dei numeri naturali che dividono 160).
   (a) Verificare che il reticolo ($\mathbf{D_{160}}$, **mcd**, **mcm**) è un reticolo limitato.
   (b) Determinare se esso è un reticolo complementato.
   (c) Disegnare il diagramma di Hasse.

(a) Il reticolo è limitato in quanto $\mathbf{mcm}(160, x) = 160$, $\mathbf{mcd}(160, x) = x$, $\mathbf{mcm}(1, x) = x$, e $\mathbf{mcd}(1, x) = 1$, per ogni x appartenente al reticolo; di conseguenza 1 e 160 sono, rispettivamente, minimo e massimo assoluti del reticolo.
(b) Il reticolo non è complementato. Infatti, l'unico elemento del reticolo tale che $\mathbf{mcd}(2, x) = 1$, è 5 e $\mathbf{mcm}(2, 5) \neq 160$; l'elemento 2 non ammette quindi un complemento.
(c) Il diagramma di Hasse è



4. Siano p, q e r forme proposizionali.
   (a) Scrivere la tavola di verità della proposizione $(q \to p) \wedge (p \to \neg r)$.
   (b) Scrivere la forma normale disgiuntiva della *negazione* di $(q \to p) \wedge (p \to \neg r)$.

(a) La tabella di verità è data da

p	q	r	$q \to p$	$p \to \neg r$	$(q \to p) \wedge (p \to \neg r)$
F	F	F	V	V	V
F	F	V	V	V	V
F	V	F	F	V	F
F	V	V	F	V	F
V	F	F	V	V	V
V	F	V	V	F	F
V	V	F	V	V	V
V	V	V	V	F	F

(b) La forma normale disgiuntiva è quindi data da

$$(\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$$