ALGEBRA E LOGICA (Geatti) Appello 5 Roma, 25 settembre 2010, ore 14-16.

Cognome ..... **Nome** .....

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare e sintetiche.*
NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 5 punti.

1. *Sia B l'insieme di tutte le soluzioni intere della congruenza* $2x \equiv 6 \bmod 8$.
   (a) Determinare B.
   (b) Richiamare la definizione di insieme numerabile.
   (c) Dimostrare che B è un insieme numerabile.

2. *Sia data la seguente la seguente informazione* $62 \cdot 61728 - 97 \cdot 39455 = 1$.
   (a) Determinare $mcd(62, 97)$, $mcd(62, 39455)$, $mcd(61728, 97)$, $mcd(61728, 39455)$ *(spiegare bene).*
   (b) Determinare $\overline{62}^{-1} \in \mathbb{Z}^*_{39455}$, $\overline{61728}^{-1} \in \mathbb{Z}^*_{39455}$, $\overline{61728}^{-1} \in \mathbb{Z}^*_{97}$, $\overline{62}^{-1} \in \mathbb{Z}^*_{97}$.
   (c) Quali altri inversi possiamo ricavare da questa informazione?

3. *Sia dato l'enunciato* $\mathcal{A} : \neg(A \vee B) \bigwedge \neg B$, *per* $A, B \in \{V, F\}$.
   (a) Usando i quantificatori $\forall$, $\exists$ *esprimere i seguenti fatti:*
   "$\mathcal{A}$ non è una tautologia", "$\mathcal{A}$ non è una contraddizione".
   (b) Usare la tabella di verità di $\mathcal{A}$ per controllare che effettivamente $\mathcal{A}$ non è né una tautologia né una contraddizione.

4. *Sia dato l'insieme* $X = \{a, b, c\}$ *e sia* $(\mathcal{P}(X), \cup, \cap, ^c)$ *l'algebra di Boole data dall'insieme delle parti di* X *munito delle operazioni di unione, intersezione e complementare.*
   (a) *Qual è la relazione d'ordine indotta su* $\mathcal{P}(X)$ *da tali operazioni? Disegnare il diagramma di Hasse associato.*
   (b) *Sia* $A = \{a, b\} \in \mathcal{P}(X)$. *Determinare tutti i maggioranti e i minoranti di* A *rispetto alla relazione d'ordine del punto (a).*
   (c) *Determinare un complemento di* A *in* $\mathcal{P}(X)$, *verificando esplicitamente la risposta.*

5. *Sia data l'espressione Booleana* $(x + y')(z + x' + yy') + (xyz')'$.
   (a) *Scriverla come somma di tutti gli implicanti primi.*
   (b) *Determinarne una forma minimale e controllare se è unica.*

6. *Il signor Rossi desidera ricevere messaggi criptati e decide di adottare il criptosistema RSA.*
   (a) *La ditta gli fornisce un kit con chiavi pubbliche* $N = 91 = 7 \cdot 13$ *ed* $E = 31$ *e chiave segreta* $D = 19$. *Vanno bene? (spiegare).*
   (b) *Preparare un kit di chiavi pubbliche* N', E' *e chiave segreta* D' *per il signor Bianchi, con* $N' = 91$ *ed* $E' = 19$.
   (c) *Il signor Verdi, che ha chiavi pubbliche* $N = 77$ *ed* $E = 13$ *e chiave privata* $D = 37$, *riceve il messaggio criptato* $m = 23$. *Decriptarlo.*