ALGEBRA E LOGICA (Geatti) 3° appello bis Roma, 16 luglio 2012, ore 10-12.

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

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

1.(a) *Richiamare la definizione di partizione di un insieme.*

.*(b) Determinare quali delle seguenti famiglie di sottoinsiemi sono partizioni di* $\mathbb{Z}$. *In caso affermativo dire quale relazione di equivalenza le determina:*

(i) $\{A_1,\ A_2\}, \qquad A_1 = \{m \in \mathbb{Z} \mid m > 0\},\ A_2 = \{m \in \mathbb{Z} \mid m < 0\}.$

(ii) $\{B_1,\ B_2\}, \qquad B_1 = \{m \in \mathbb{Z} \mid \exists k \in \mathbb{Z} :\ \ m = 2k\},\ B_2 = \{m \in \mathbb{Z} \mid \exists k \in \mathbb{Z} :\ \ m = 2k+1\}.$

.*(c) Esibire la partizione di* $\mathbb{Z}$ *associata alla seguente relazione di equivalenza:*
dati $x, y \in \mathbb{Z}$, $\quad xRy$ *se e solo se* $x \equiv y \bmod 3$.

Sol. (a) Vedi dispense sulle relazioni (relazioni di equivalenza).
(b) La famiglia in (i) non è una partizione di $\mathbb{Z}$ perché $A_1 \cup A_2 \neq \mathbb{Z}$: infatti $0 \notin A_1 \cup A_2$; la famiglia in (ii) è una partizione di $\mathbb{Z}$: infatti i sottoinsiemi B_1 e B_2 sono non vuoti e disgiunti. Inoltre $B_1 \cup B_2 = \mathbb{Z}$. La relazione di equivalenza le cui classi di equivalenza sono i sottoinsiemi B_1 e B_2 è la relazione di congruenza modulo 2:

$$m, n \in Z \quad mRn \quad \Leftrightarrow \quad m \equiv n \bmod 2.$$

infatti $B_1 = \{m \in \mathbb{Z} \mid m \equiv 0 \bmod 2\}$, cioè l'insieme degli interi pari, mentre $B_2 = \{m \in \mathbb{Z} \mid m \equiv 1 \bmod 2\}$, cioè l'insieme degli interi dispari.
(c) La partizione di $\mathbb{Z}$ associata alla congruenza modulo 3 è formata appunto dalle tre classi resto modulo 3:

$$\{A_0, A_1, A_2\},$$

con

$$A_0 = \{m \in \mathbb{Z} \mid m \equiv 0 \bmod 3\} = \{m = 3k,\ k \in \mathbb{Z}\},$$
$$A_1 = \{m \in \mathbb{Z} \mid m \equiv 1 \bmod 3\} = \{m = 1 + 3k,\ k \in \mathbb{Z}\},$$
$$A_2 = \{m \in \mathbb{Z} \mid m \equiv 2 \bmod 3\} = \{m = 2 + 3k,\ k \in \mathbb{Z}\}.$$

2.(a) *Esibire due insiemi infiniti distinti* A *e* B *(a piacere) tali che l'intersezione* $A \cap B$ *sia finita.*

.*(b) Esibire due insiemi infiniti distinti* A *e* B *(a piacere) tali che l'intersezione* $A \cap B$ *sia numerabile.*

.*(c) Esibire due insiemi infiniti distinti* A *e* B *(a piacere) tali che l'intersezione* $A \cap B$ *sia non numerabile.*
Giustificare bene le risposte.

Sol. Ci sono infiniti modi di risponedere a queste domande. Ad esempio
(a) $A = \{m \in \mathbb{Z} \mid m \leq 10\}, \quad B = \{m \in \mathbb{Z} \mid m \geq -10\}, \quad A \cap B = \{-10, -9, \ldots, 9, 10\}$.
(b) $A = \mathbb{Z}, \quad B = \mathbb{N} \subset \mathbb{Z}, \quad A \cap B = \mathbb{N}$.
(c) $A = (0, 2), \quad B = (0, 1) \subset A, \quad A \cap B = (0, 1)$. Come abbiamo visto in classe, $(0, 1)$ non è numerabile.

3.(a) *Esibire un esempio di funzione* $f\colon \mathbb{Z} \to \mathbb{Z}$ *che sia iniettiva e non suriettiva.*

.*(b) Esibire un esempio di funzione* $f\colon \mathbb{Z} \to \mathbb{Z}$ *che sia suriettiva e non iniettiva*

.*(c) Esibire un esempio di funzione* $f\colon \mathbb{Z} \to \mathbb{Z}$, *diversa dall'identità, che sia biiettiva.*
Giustificare bene le risposte.

Sol. Ci sono infiniti modi di risponedere a queste domande. Ad esempio
(a) $f\colon \mathbb{Z} \to \mathbb{Z}, \quad m \mapsto 2m$.
f è iniettiva: $2m = 2n \ \Rightarrow\ m = n$;
l'immagine $f(\mathbb{Z})$ coincide con gli intero pari. Dunque f non è suriettiva.

(b) $f\colon \mathbb{Z} \to \mathbb{Z}, \quad m \mapsto \begin{cases} m/2 & m \text{ pari} \\ (m-1)/2 & m \text{ dispari.} \end{cases}$

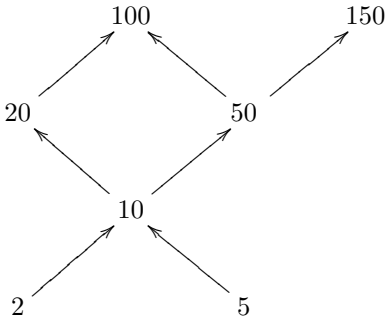
f è suriettiva: m pari significa che esiste $k \in \mathbb{Z}$ per cui $m = 2k$. Questa formula dà una corrispondenza biunivoca tra $\mathbb{Z}$ ed i numeri pari. Quindi f è suriettiva (l'immagine dei numeri pari copre già tutto $\mathbb{Z}$). Analogamente m dispari significa che esiste $h \in \mathbb{Z}$ per cui $m = 2h-1$. Questa formula dà una corrispondenza biunivoca tra $\mathbb{Z}$ ed i numeri dispari. Quindi anche l'immagine dei numeri dispari copre tutto $\mathbb{Z}$. Dunque f non è iniettiva. Si può anche verficare che $f(6) = f(7) = 3$.
(c) $f\colon \mathbb{Z} \to \mathbb{Z}, \quad m \mapsto m+1$ è biiettiva. f è iniettiva: $m = 1 = n+1 \ \Rightarrow m = n$; inoltre ogni $k \in \mathbb{Z}$ appartiene all'immagine di f: infatti $k = f(k-1)$.

4.(a) *Calcolare* $mcd(11111, 1111)$ *(esibire i passaggi).*
(b) Determinare se 10 *ammette o meno inverso moltiplicativo in* $\mathbb{Z}^*_{1001}$*, spiegando bene perché.*
(c) Sapendo che $24 \cdot 127 - 11 \cdot 277 = 1$*, determinare* $\overline{24^{-1}}$ mod 277*.*

Sol. (a) $11111 = 10 * 1111 + 1$. Quindi $mcd(11111, 1111) = 1$. Il resto successivo nell'algoritmo di Euclide sarebbe necessariamente 0!.
(b) 10 ammette inverso moltiplicativo in $\mathbb{Z}^*_{1001}$ se e solo se $mcd(10, 1001) = 1$. Abbiamo che $10 = 2 * 5$. Poiché 41001 non è divisibile né per 2 né per 5, si ha che $mcd(10, 1001) = 1$. Dunque 10 ammette inverso moltiplicativo in $\mathbb{Z}^*_{1001}$.
(c) Poiché $24 \cdot 127 - 11 \cdot 277 = 1$, si ha che $24 \cdot 127 \equiv 1$ mod 277. Dunque $\overline{24^{-1}} = \overline{127}$ mod 277.

5. *Sia dato l'insieme* $X = \{2, 5, 10, 20, 50, 100, 150\}$ *con l'ordinamento parziale dato dalla divisibilità:*
dati $m, n \in X$, $\quad m \leq n \quad$ *se* $\quad m \mid n \quad$ *(cioè se* m *divide* n*).*
(a) Disegnare il diagramma di Hasse di $(X, \leq)$*.*
(b) Richiamare le definizioni di elementi minimali e massimali, e di massimo e minimo.
(c) Determinare elementi minimali e massimali, ed eventuali massimo e minimo di X*.*
(d) Determinare l'insieme dei maggioranti e l'insieme dei minoranti di $A = \{50\}$*.*

Sol. (a)



(b) Vedi dispense sulle relazioni di ordine.
(c) L'insieme X non ha minimo né massimo : nessun elemento è $\leq$ di tutti gli altri, e non c'è nessun elemento M con la proprietà che $x \leq M$, per ogni $x \in X$. Invece ha X ha due elementi minimali $\{2, 5\}$ e due elementi massimali $\{100, 150\}$.
(d) $Magg(A) = \{x \in X : \ 50 \leq x\} = \{50, 100, 150\}$; $\quad min(A) = \{x \in X : \ x \leq 50\} = \{2, 5, 10, 50\}$.

6. *Sia data l'espressione Booleana* $\quad E(x, y, z) = (x + y')'(z + x' + yy')' + (x'yz')$.
(a) Scrivere E *come somma di tutti gli implicanti primi.*
(b) Determinarne una forma minimale di E *e controllare se è unica.*

Sol. Usando $(xy)' = x' + y'$, $\quad (x')' = x$, $\quad xx' = 0$, troviamo

$$E(x, y, z) = (x + y')'(z + x' + yy')' + (x'yz') = (x'y)(z + x' + 0)' + (x'yz') = x'yz'x + (x'yz') =$$

$$= 0 + x'yz' = x'yz'.$$

Il metodo del consenso non ha mosse, quindi abbiamo scritto E come somma di tutti gli implicanti primi. Il fatto che questa forma sia minimale dipende dal fatto che ha un solo monomio non semplificabile; che sia unica segue dal fatto che tale monomio è completo (contiene tutte le variabili).