ALGEBRA E LOGICA (Geatti) 5° appello Roma, 25 settembre 2009, ore 11–13.

**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. *Determinare tutti i numeri naturali di due cifre decimali che divisi per 5 danno resto 2 e divisi per 7 danno resto 4.*

*Sol.* Dobbiamo determinare i numeri interi $10 \leq x \leq 99$ che sono soluzioni del sistema di congruenze

$$\begin{cases} x \equiv 2 \bmod 5 \\ x \equiv 4 \bmod 7. \end{cases}$$

Osserviamo innanzitutto che le due congruenze ammettono singolarmente soluzioni intere e cosı' pure il sistema, poiché $mcd(5,7) = 1$. Inoltre per il Teorema Cinese del Resto tutte le soluzioni intere del sistema sono della forma $x = x_0 + 35M$, dove $x_0$ è una soluzione particolare ed $M$ varia in $\mathbb{Z}$ (la soluzione è "unica" modulo 35). Sostituendo la soluzione generale della prima congruenza $x = 2 + k5,\ k \in \mathbb{Z}$, nella seconda troviamo l'equazione diofantea

$$2 + 5k = 4 + 7h \quad \Leftrightarrow \quad 5k - 7h = 2. \qquad (*)$$

La soluzione generale dell'equazione (*) è $(k,h) = (-1+7M, -1+5M)$, al variare di $M \in \mathbb{Z}$. La coordinata $k = -1+7M,\ M \in \mathbb{Z}$, sostituita nella soluzione generale della prima congruenza, ci dà la soluzione generale del sistema

$$x = 2 + 5(-1 + 7M) = -3 + 35M = 32 + 35M, \quad M \in \mathbb{Z}.$$

I numeri interi $10 \leq x \leq 99$ che sono soluzioni del sistema sono precisamente $x = 32$ e $x = 67$.

2. *Siano $A$ e $B$ due insiemi e sia $f\colon A \to B$ una funzione.*
   *(a) Richiamare la definizione di funzione iniettiva e di funzione suriettiva.*
   *(b) Sia $f\colon \mathbb{N} \to \mathbb{Z}$ data da $f(n) = n^2$, dove $\mathbb{N} = \{1, 2, 3 \ldots\}$ e $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$. Determinare se $f$ è iniettiva e se è suriettiva. Spiegare bene la risposta.*
   *(c) Siano $A = \mathbb{N}$ e $B = \mathbb{Z}$, oppure $B = \mathcal{P}(\mathbb{N})$, oppure $B = \mathbb{R}$, oppure $B = \mathcal{P}(\{a,b,c\})$. Esiste una funzione biiettiva $f\colon A \to B$? Spiegare bene la risposta.*

*Sol.* (a) Vedi un testo qualunque...

(b) Iniettività: Supponiamo che valga $f(n) = f(m)$, ossia $n^2 = m^2$. Poiché $n, m > 0$, ciò implica $n = m$. Dunque $f$ è iniettiva.
Suriettività: l'applicazione non è suriettiva. Ad esempio nessun numero intero negativo è il quadrato di un numero naturale. Ma anche fra i numeri interi positivi ce ne sono infiniti che non sono quadrati di un numero naturale: ad esempio 5,7, 8, etc...

(c) $A = \mathbb{N}$ e $B = \mathbb{Z}$ hanno la stessa cardinalità. $\mathbb{Z}$ è un insieme numerabile: per definizione esiste una funzione biiettiva $f\colon \mathbb{N} \to \mathbb{Z}$;
$A = \mathbb{N}$ e $B = \mathcal{P}(\mathbb{N})$ non hanno la stessa cardinalità (dato un insieme $A$, l'insieme delle parti $\mathcal{P}(A)$ ha sempre cardinalità superiore a quella di $A$), pertanto non esiste una funzione biiettiva $f\colon \mathbb{N} \to \mathcal{P}(\mathbb{N})$;
$A = \mathbb{N}$ e $B = \mathbb{R}$ non hanno la stessa cardinalità ($\mathbb{R}$ non è numerabile), pertanto non esiste una funzione biiettiva $f\colon \mathbb{N} \to \mathbb{R}$ ;
$A = \mathbb{N}$ e $B = \mathcal{P}(\{a,b,c\})$ non hanno la stessa cardinalità ($\mathcal{P}(\{a,b,c\})$ ha cardinalità finita, uguale a 8), pertanto non esiste una funzione biiettiva $f\colon \mathbb{N} \to \mathcal{P}(\{a,b,c\})$.

3. *Il signor Rossi desidera ricevere messaggi criptati e decide di adottare il criptosistema RSA. La ditta gli fornisce un kit con chiavi pubbliche $N$ ed $E$ e chiave segreta $D$.*
   *(a) La ditta gli fornisce un kit con chiavi pubbliche $N = 143$ ed $E = 23$ e chiave segreta $D = 3$. Vanno bene? (spiegare).*
   *(b) Preparare un kit di chiavi pubbliche $N'$, $E'$ e chiave segreta $D'$ per il signor Bianchi, con $N' = 77$ ed $E' = 7$.*

*(c) Spedire a Verdi, con chiavi pubbliche $N = 77$ ed $E = 7$, il messaggio $m = 13$ dopo averlo criptato.*

*Sol.* (a) Il numero $N$ si fattorizza come $N = p \cdot q$ con $p = 11$ e $q = 13$. In questo caso $(p-1)(q-1) = 10 \cdot 12 = 120$. La chiave $E = 23$ soddisfa $mcd(23, 120) = 1$. Dunque appartiene a $Z^*_{120}$, come deve essere. Invece la chiave $D = 3$ non appartiene $Z^*_{120}$, in quanto $mcd(3, 120) = 3 \neq 1$. Inoltre $E \cdot D = \overline{69} \neq \bar{1}$ in $Z^*_{120}$. Conclusione questo kit non va bene.
(b) Il numero $N'$ si fattorizza come $N' = p' \cdot q'$ con $p' = 7$ e $q' = 11$. In particolare $(p-1)(q-1) = 60$. La chiave $E' = 7$ soddisfa $mcd(7, 60) = 1$, quindi appartiene a $\mathbb{Z}^*_{60}$ come deve. La chiave segreta $D'$ è l'inverso di $E'$ modulo 60, ossia: $D' = (7)^{-1}$ modulo 60. Risolvendo l'equazione diofantea $7D' + k60 = 1$ con l'algoritmo di Euclide si trova $D' = 43$.
(c) Osserviamo innanzitutto che $mcd(m, N) = mcd(13, 77) = 1$ come deve essere. Il messaggio $m = 13$ criptato con chiavi pubbliche $N = 77$ ed $E = 7$ è dato $m^E \mod N$, ossia $13^7 = 62 \mod 77$.

4. *Siano dati i reticoli* $(D_{24}, \text{mcd}, \text{mcm})$ *e* $(D_{30}, \text{mcd}, \text{mcm})$.
   *(a) Determinare l'ordinamento di ordine parziale indotto sui reticoli dalle operazioni di* mcd *e* mcm *e disegnare i rispettivi diagrammi di Hasse.*
   *(b) Deteminare se i due reticoli sono o meno isomorfi, spiegando bene la risposta.*

*Sol.* (a) $\mathbf{D}_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$ e $\mathbf{D}_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$. In questi reticoli l'ordinamento di ordine parziale indotto sui reticoli dalle operazioni di mcd e mcm è il seguente: $m$" $\leq$ "$n$ se $\text{mcd}(m, n) = m$ oppure se $\text{mcm}(m, n) = n$. Questo equivale a dire $m$" $\leq$ "$n$ se $m$ divide $n$.

Diagrammi di Hasse: ....

(b) Pur avendo lo stesso numero di elementi, i due reticoli non sono isomorfi: $D_{30}$ è un'algebra di Boole (30 è prodotto di primi distinti) mentre $D_{24}$ no. Si può anche verificare direttamente che non esiste una funzione biiettiva fra i due reticoli che rispetta l'ordinamento (vedi soluzioni esercizi foglio 6).

5. *Siano dati gli enunciati* $A \wedge (\neg B \vee \neg A) \vee (A \Rightarrow B)$ *e* $A \vee (\neg B \wedge \neg A) \vee (A \wedge \neg B)$.
   *(a) Scrivere enunciati ad essi equivalenti in forma normale disgiuntiva.*
   *(b) Determinare se si tratta di enunciati logicamente equivalenti.*

*Sol.* (a) $A \wedge (\neg B \vee \neg A) \vee (A \Rightarrow B) \quad \Leftrightarrow \quad (A \wedge \neg B) \bigvee (A \wedge \neg A) \bigvee \neg A \vee B \quad \Leftrightarrow \quad (A \wedge \neg B) \bigvee \neg A \bigvee B$;
nel primo passaggio abbiamo usato la proprietà distributiva; nel secondo il fatto che $(A \wedge \neg A)$ è una contraddizione e dunque in nella forma normale disgiuntiva (somma di prodotti) porta contributo nullo. Il secondo enunciato è già in forma normale disgiuntiva.

(b) Dalla tabella di verità si vede che il primo enunciato è una tautologia, ossia è vero per ogni valore di $A$ e $B$. Il secondo enunciato non è sempre vero: ad esempio è falso se $A$ è falso e $B$ è vero. Conclusione: i due enunciati non sono logicamente equivalenti.

6. *Considerare il seguente enunciato*

$$\forall n \in \mathbb{N} \quad \exists a \in \mathbb{Z} \quad \exists b \in \mathbb{Z} \quad n = 5a + b.$$

   *(a) Determinare se l'enunciato è vero o meno (motivare bene la risposta).*
   *(b) Negare l'enunciato (N.B. non ci devono essere negazioni davanti ai quantificatori).*

*Sol.* (a) L'enunciato in sostanza dice che ogni numero naturale è somma di due interi, di cui il primo è un multiplo intero di 5. L'enunciato è vero: fissato $n$, basta prendere ad esempio $a = 0$ e $b = n$.

(b) La negazione dell'enunciato è:

$$\exists n \in \mathbb{N} \quad \forall a \in \mathbb{Z} \quad \forall b \in \mathbb{Z} \quad n \neq 5a + b.$$

Se l'enunciato originale è vero, la sua negazione è un enunciato falso.