ALGEBRA E LOGICA (Geatti) 2° appello Roma, 2 marzo 2010, ore 10:00–12:00.

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 X un insieme e sia $\mathcal{P}(X)$ l'insieme delle parti di X. Sia R la relazione su $\mathcal{P}(X)$ così definita: dati $A, B \in \mathcal{P}(X)$, diciamo che $A\ R\ B$ se $A \cup B = X$.*
(a) Determinare se la relazione R è riflessiva, simmetrica, antisimmetrica o transitiva (per ognuna di queste proprietà, verificare che vale oppure esibire almeno una coppia A, B per cui non vale).

R non è riflessiva: per ogni $A \in \mathcal{P}(X)$ con $A \neq X$ si ha $A \cup A = A \neq X$. Dunque non è vero che A è in relazione con A, per ogni $A \in \mathcal{P}(X)$;
R è simmetrica: se vale $A \cup B = X$ allora vale anche $B \cup A = X$. Dunque ARB implica BRA;
R non è antisimmetrica: dati $A, B \in \mathcal{P}(X)$ con $\begin{cases} A \cup B = X \\ B \cup A = X \end{cases}$, in generale NON NE SEGUE che $A = B$.

Prendiamo ad esempio $X = \{a, b, c\}$. Gli elementi $A = \{a, b\}$ e $B = \{b, c\} \in \mathcal{P}(X)$ soddisfano $A \cup B = X$ e $B \cup A = X$, ma $A \neq B$.
R non è transitiva: dati $A, B, C \in \mathcal{P}(X)$ con $\begin{cases} A \cup B = X \\ B \cup C = X \end{cases}$, in generale NON NE SEGUE che $A \cup C = X$.

Prendiamo ad esempio $X = \{a, b, c\}$. Gli elementi $A = \{a\}$, $B = \{b, c\}$ e $C = \{a, c\} \in \mathcal{P}(X)$ soddisfano $A \cup B = X$, $B \cup C = X$ ma $A \cup C \neq X$.

2. (a) *Determinare tutte le soluzioni intere del sistema di congruenze* $\begin{cases} x \equiv 1 \bmod 7 \\ x \equiv 4 \bmod 9. \end{cases}$
(b) *Determinare le soluzioni comprese nell'intervallo* $[0, 100]$.

(a) Poiché le singole congruenze hanno soluzioni intere e $mcd(7, 9) = 1$, per il Teorema Cinese del Resto anche il sistema ammette soluzioni intere. Tali soluzioni sono della forma $x = x_0 + 63N$, dove x_0 è una soluzione particolare ed N varia in $\mathbb{Z}$. Sostituendo le soluzioni della prima congruenza $x = 1 + 7k,\ k \in \mathbb{Z}$ nella seconda, troviamo la congruenza in k

$$1 + 7k \equiv 4 \bmod 9 \quad \Leftrightarrow \quad 7k \equiv 3 \bmod 9. \qquad (*)$$

Gli interi k che soddisfano (*) parametrizzano precisamente le soluzioni della prima congruenza che sono anche soluzioni della seconda: in altre parole le soluzioni del sistema. Troviamo

$$7k \equiv 3 \bmod 9 \quad \Leftrightarrow \quad k = 3 + 9N,\ N \in \mathbb{Z}$$

da cui le soluzioni del sistema risultano

$$x = 1 + 7(3 + 9N) = 22 + 63N, \quad N \in \mathbb{Z}.$$

(b) Le soluzioni del sistema comprese nell'intervallo $[0, 100]$ sono $x = 22$ (per $N = 0$) ed $x = 85$ (per $N = 1$).

3. (a) *Enunciare il Teorema di Lagrange per un gruppo abeliano finito G di cardinalità $\#G = n$.*
(b) Elencare gli elementi di $\mathbb{Z}_{21}^*$ ed enunciare il Teorema di Lagrange per $G = \mathbb{Z}_{21}^*$.
(c) Sia $\bar{x} = \bar{5}^{11} \in \mathbb{Z}_{21}^*$. Chi è $\bar{x}^{-1}$?

(a) Sia G un gruppo abeliano finito di cardinalità $\#G = n$. Allora $g^n = g \cdot g \cdot \ldots \cdot g = e$, per ogni $g \in G$. Vedi nota2.
(b) Osserviamo innanzitutto che la cardinalità di $\mathbb{Z}_{21}^*$ è $\varphi(21) = \varphi(3)\varphi(7) = 2 \cdot 6 = 12$. Precisamente $\mathbb{Z}_{21}^* = \{\bar{x} \in \mathbb{Z}_{21} \mid \mathrm{mcd}(x, 21) = 1\} = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{8}, \overline{10}, \overline{11}, \overline{13}, \overline{16}, \overline{17}, \overline{19}, \overline{20}\}$. In questo caso il Teorema di Lagrange dice che:
$\forall \bar{x} \in \mathbb{Z}_{21}^*, \quad \bar{x}^{12} = \bar{1}$ in $\mathbb{Z}_{21}^*$. In altre parole, $\forall x$ con $mcd(x, 21) = 1$, vale $x^{12} \equiv 1 \bmod 21$.
(c) Poiché $\bar{5} \in \mathbb{Z}_{21}^*$ e $\bar{5}^{12} = \bar{5}^{11} \cdot \bar{5} = \bar{1}$, ne segue che $(\bar{5}^{11})^{-1} = \bar{5}$.

4. *Il signor Rossi ha un kit RSA con chiavi pubbliche* $N = 143 = 11 \cdot 13$ *ed* $E = 7$.
   (a) Spedire a Rossi il messaggio $m = 3$ *dopo averlo criptato.*
   (b) Il signor Bianchi ha un kit RSA con chiavi pubbliche $N = 143 = 11 \cdot 13$ *ed* $E = 17$. *Costruirgli la chiave segreta* D.

(a) Spediamo al signor Rossi $\bar{m}^E \bmod N$, cioè

$$\bar{3}^7 = \bar{3}^5 \cdot \bar{3}^2 = \overline{243} \cdot \bar{9} = \overline{100} \cdot \bar{9} = \overline{42} \bmod 143.$$

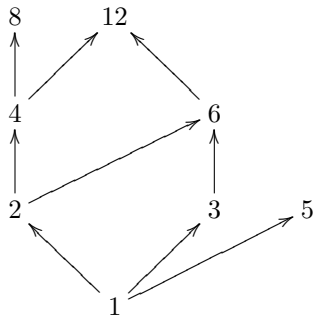
(b) Se $N = p \cdot q$, la chiave D è data da $D = E^{-1} \bmod (p-1)(q-1)$. Nel nostro caso $p = 11$, $q = 13$ e $(p-1)(q-1) = 120$. Mediante l'algoritmo di Euclide esteso .... troviamo

$$D = 17^{-1} \bmod 120, \qquad D = 113.$$

Prova: $17 \cdot 113 = 1921 \equiv 1 \bmod 120$.

5. *Sia dato l'insieme* $X = \{1, 2, 3, 4, 5, 6, 8, 12\}$ *con la relazione di ordine parziale data da:* aRb *se* a *divide* b.
   (a) Disegnare il diagramma di Hasse di (X, R).
   (b) Sia dato il sottoinsieme $A = \{1, 2, 4\} \subset X$. *Determinare, se esistono, maggioranti, minoranti, massimo e minimo di* A *(in caso affermativo, elencarli).*
   (c) Dire se (X, R) *è un reticolo, spiegando la risposta.*

(a)



(b) I maggioranti di A sono l'insieme $maggior(A) = \{4, 8, 12\}$: infatti tutti gli elementi di A dividono 4,8,12. Il minimo dei maggioranti di A, cioè 4, è l'estremo superiore di A e anche il massimo di A, visto che appartiene ad A.
I minoranti di A sono l'insieme $minor(A) = \{1\}$: infatti 1 divide tutti gli elementi di A. Il massimo dei minoranti di A, cioè 1, è l'estremo inferiore di A e anche il minimo di A, visto che appartiene ad A.
(c) Un reticolo è un insieme parzialmente ordinato che contiene $\inf(a, b)$ e $\sup(a, b)$, per ogni coppia $a, b \in X$. Nel nostro caso $\inf(a, b) = \mathrm{mcd}(a, b)$ e $\sup(a, b) = \mathrm{mcm}(a, b)$. È chiaro che X non è un reticolo: ad esempio $\mathrm{mcm}(5, 8) = 40 \notin X$.

6. *Considerare il seguente enunciato* $\mathcal{A}$: $\forall (x, y) \in \mathbb{R}^2 \quad (xy > 0) \bigvee (xy = 0)$.
   (a) Determinare se l'enunciato $\mathcal{A}$ *è vero o falso, spiegando bene la risposta.*
   (b) Formulare l'enunciato $\neg\mathcal{A}$ *(non ci devono essere negazioni davanti ai quantificatori).*

(a) L'enunciato $\mathcal{A}$ è falso: infatti per ogni $(x, y) \in \mathbb{R}^2$, con x, y non nulli di segno discorde, vale $xy < 0$. Ad esempio $\mathcal{A}$ è falso per $x = 1$ e $y = -1$.
(b) $\neg\mathcal{A}$:

$$\exists (x, y) \in \mathbb{R}^2 \quad \neg((xy > 0) \bigvee (xy = 0)) \quad \Leftrightarrow$$

$$\exists (x, y) \in \mathbb{R}^2 \quad \neg(xy > 0) \bigwedge \neg(xy = 0) \quad \Leftrightarrow$$

$$\exists (x, y) \in \mathbb{R}^2 \quad (xy \leq 0) \bigwedge (xy \neq 0) \quad \Leftrightarrow$$

$$\exists (x, y) \in \mathbb{R}^2 \quad xy < 0.$$

Come anticipato al punto precedente, $(x, y) = (1, -1)$ rende vera $\neg\mathcal{A}$.