Algebra e Logica 2015 (Geatti-Iannuzzi) 3° appello Roma, 23 giugno 2016, 15:00–17:00.

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. *Determinare tutte le soluzioni intere del sistema di congruenze* $\begin{cases} x \equiv 2 \bmod 6 \\ x \equiv 5 \bmod 9 \end{cases}$. *Disegnarle sulla retta reale.*

Sol.: (a) Evidentemente le congruenze del sistema singolarmente ammettono soluzioni intere. Le soluzioni della prima congruenza sono gli interi della forma

$$x = 2 + 6k, \quad \text{al variare di } k \in \mathbf{Z}. \tag{$*$}$$

Sostituendole nella seconda, troviamo

$$2 + 6k = 5 + 9h \quad \Leftrightarrow \quad 6k - 9h = 3 \quad \Leftrightarrow \quad 2k - 3h = 1, \quad k, h \in \mathbf{Z}. \tag{$**$}$$

Poiché $mcd(2, 3) = 1$ (!!), le soluzioni dell'equazione diofantea (**) sono le coppie di interi

$$(k, h) = (-1, -1) + (3M, 2M), \quad \text{al variare di } M \in \mathbf{Z}.$$

Il significato delle soluzioni dell'equazione diofantea (**) è questo: gli interi $k = -1+3M$, $M \in \mathbf{Z}$, parametrizzano le soluzioni della prima congruenza che sono anche soluzioni della seconda, e dunque soluzioni del sistema.

Conclusione: le soluzioni del sistema dato sono gli interi

$$x = 2 + 6(-1 + 3M) = -4 + 18M = 14 + 18M, \quad \text{al variare di } M \in \mathbf{Z}.$$

2. *Sia R la relazione su $\mathcal{P}(X)$, l'insieme delle parti di un insieme X, definita così :*
   "ARB se e solo se $A \cap B \neq \emptyset$".
   (a) Determinare se si tratta o meno di una relazione di equivalenza su $\mathcal{P}(X)$.
   (b) Determinare quali dei seguenti elementi $\{x, y\}, \{x\}, \{y, z\}, \{z\}, \emptyset$ di $\mathcal{P}(\{x, y, z\})$ sono in relazione fra loro.

Sol.: (a)
- *Riflessività:* la relazione R *non* è riflessiva perché $\emptyset \in \mathcal{P}(X)$, ma $\emptyset \cap \emptyset = \emptyset$.
- *Simmetria:* la relazione R è simmettrica perché $A \cap B \neq \emptyset$ implica $B \cap A \neq \emptyset$.
- *Transitività:* la relazione R *non* è transitiva perché $\begin{cases} A \cap B \neq \emptyset \\ B \cap C \neq \emptyset \end{cases}$ *non* implica $A \cap C \neq \emptyset$.

Ad esempio basta prendere $A = \{x, y\}$, $B = \{y, z\}$, $C = \{z\}$.
In conclusione, R non è una relazione di equivalenza.

(b) Ognuno degli elementi dati è in relazione con se stesso, eccetto per l'insieme vuoto. Inoltre

$$\{x, y\}R\{x\}, \quad \{x, y\}R\{y, z\}, \quad \{y, z\}R\{z\}$$

e per simmetria

$$\{x\}R\{x, y\}, \quad \{y, z\}R\{x, y\}, \quad \{z\}R\{y, z\}.$$

3. *Verificare che $3^{32} - 2^{32}$ è divisibile per 13 (senza usare numeri con più di due cifre...e spiegando i principi usati).*

Sol.: Dobbiamo verificare che

$$3^{32} - 2^{32} \equiv 0 \bmod 13.$$

Poiché 13 è primo, per il Piccolo Teorema di Fermat,

$$3^{12} \equiv 2^{12} \equiv 1 \bmod 13.$$

Di conseguenza

$$3^{32} - 2^{32} \equiv 3^8 - 2^8 \equiv 3^3 3^3 3^2 - 2^4 2^4 \equiv 1 \cdot 1 \cdot 9 - 3 \cdot 3 \equiv 0 \bmod 13.$$

4. *Per ricevere messaggi criptati, il signor Rossi adotta il criptosistema RSA con chiavi pubbliche N ed E e chiave segreta D (nelle domande (b) e (c) non è necessario svolgere i calcoli).*
   (a) Determinare E, sapendo che $N = 65$ e $D = 5$.
   (b) Il signor Rossi riceve il messaggio criptato $m = 33$. Che cosa calcola per decriptarlo?
   (c) Che cosa si calcola per criptare il messaggio $m = 31$ da inviare al signor Rossi?

Sol.: (a) Il numero N si fattorizza come $N = p \cdot q$ con $p = 5$ e $q = 13$. In questo caso $(p-1)(q-1) = 4 \cdot 12 = 48$. La chiave $D = 5$ soddisfa $mcd(5, 48) = 1$. Dunque appartiene a Z_{48}^*, come deve essere. La chiave E è data da $E \equiv D^{-1} \equiv 5^{-1} \bmod 48$. Per calcolarla applichiamo l'algoritmo di Euclide esteso. Da

$$48 = 9 \cdot 5 + 3, \quad 5 = 1 \cdot 3 + 2, \quad 3 = 1 \cdot 2 + 1.$$

$$1 \cdot 48 + 0 \cdot 5 = 48, \quad 0 \cdot 48 + 1 \cdot 5 = 5;$$

Sottraendo 9 volte la seconda relazione dalla prima, troviamo

$$1 \cdot 48 + (-9) \cdot 5 = 3;$$

sottraendo la terza relazione dalla seconda troviamo

$$(-1) \cdot 48 + 10 \cdot 5 = 2.$$

Infine sottraendo la quarta relazione dalla terza troviamo

$$2 \cdot 48 + (-19) \cdot 5 = 1.$$

Dunque $\overline{5}^{-1} = \overline{-19} = \overline{29}$ in Z_{48}^* (si può verificare che $5 \cdot 29 = 145 \equiv 1 \bmod 48$). La chiave cercata è $E = 29$.
(b) Per descriptare il messaggio criptato $m = 19$, Rossi calcola $m^D \bmod N$, ossia $19^5 \bmod 65$.
(c) per criptare il messaggio $m = 23$ da inviare al signor Rossi, si calcola $m^E \bmod N$, ossia $23^{29} \bmod 65$.

5. *Sia D_{36} l'insieme dei divisori di 36 con la relazione di ordine parziale data dalla divisibilità: aRb se $a \mid b$. Sia $S = \{4, 6\} \subset D_{36}$.*
   (a) Con quali elementi di D_{36} è in relazione 6?
   (b) Determinare tutti i maggioranti e tutti i minoranti di S in D_{36}.
   (c) Determinare, se esistono, $\inf(S)$, $\sup(S)$, $max(S)$, $min(S)$.

Sol.: $D_{36} = \{1, 2, 4, 3, 6, 9, 12, 18, 36\}$.
(a) Per definizione, $6Rx$ se $6|x$, per cui

$$6R6, \quad 6R12, \quad 6R18, \quad 6R36.$$

(b) Per definizione x è un maggiorante di S se $4|x$ & $6|x$, per cui

$$magg(S) = \{12, 36\}$$

Per definizione x è un minorante di S se $x|4$ & $x|6$, per cui

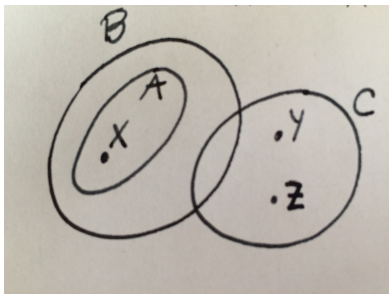
$$minor(S) = \{1, 2\}.$$

(c) $sup(S)$=minimo dei maggioranti=12;
$inf(S)$=massimo dei minoranti=2;
Poiché $sup(S)$ e $inf(S)$ non appartengono ad S, l'insieme S non ha né massimo né minimo.

6. *A partire dalla figura qui sotto, determinare quali delle seguenti affermazioni sono vere*

(1) $(x \in A) \bigwedge \neg(x \in B)$; (2) $(y \in B \setminus C) \bigvee \neg(x \in C)$;

(3) $(x \in A) \bigwedge ((y \in A) \vee (z \in A))$; (4) $x \in A \Rightarrow (x \in B) \vee (x \in C)$.



Sol.: La (1) è falsa, perche' $A \subset B$ e quindi un elemento di A è anche un elemento di B;
la (2) è vera, perche' almeno una delle due affermazioni è vera, ossia $x \notin C$.
la (3) è falsa, perché $(y \in A) \vee (z \in A)$ è falsa: né y né z appartengono ad A;
la (4) è vera, perche' $x \in A$ è vera ed anche $(x \in B) \vee (x \in C)$ è vera (è vera $(x \in B)$).