Algebra e Logica 2015 (Geatti) 1° appello Roma, 27 gennaio 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.(a) *Determinare tutte le soluzioni intere del sistema di congruenze* $\begin{cases} x \equiv 3 \bmod 6 \\ x \equiv 3 \bmod 9. \end{cases}$

(b) Determinare tutte le soluzioni comprese nell'intervallo $[0, 25]$.

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

$$x = 3 + 6k, \quad \text{al variare di } k \in \mathbf{Z}. \tag{$*$}$$

Sostituendole nella seconda, troviamo

$$3 + 6k = 3 + 9h \quad \Leftrightarrow \quad 6k - 9h = 0 \quad \Leftrightarrow \quad 2k - 3h = 0, \quad k, h \in \mathbf{Z}. \tag{$**$}$$

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

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

Il significato delle soluzioni dell'equazione diofantea (**) è questo: gli interi $k = 3M$, $M \in \mathbf{Z}$, 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

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

(b) Le soluzioni del sistema comprese nell'intervallo $[0, 25]$ sono $x = 3$ (per $M = 0$) e $x = 21$ (per $M = 1$).

2. *Sia A insieme con 3 elementi. Determinare la cardinalità dei seguenti insiemi*

$$A \cap (A \setminus A), \qquad A \cup (A \cap A), \qquad A \cup \mathcal{P}(A), \qquad \mathcal{P}(A) \times \mathcal{P}(A), \qquad \mathcal{P}(A \times A).$$

Sol.: Sia $A = \{a, b, c\}$. Allora $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A = \{a, b, c\}\}$ e vale $|\mathcal{P}(A)| = 2^{|A|}$.

1. $A \cap (A \setminus A) = A \cap \emptyset = \emptyset$, per cui $|A \cap (A \setminus A)| = 0$;
2. $A \cup (A \cap A) = A \cup A = A$, per cui $|A \cup (A \cap A)| = 3$;
3. $|A \cup \mathcal{P}(A)| = |A| + |\mathcal{P}(A)| = 3 + 8 = 11$;
4. $\mathcal{P}(A) \times \mathcal{P}(A) = \{(X, Y) \mid X, Y \in \mathcal{P}(A)\}$, da cui $|\mathcal{P}(A) \times \mathcal{P}(A)| = |\mathcal{P}(A)| \cdot |\mathcal{P}(A)| = 8 \cdot 8 = 64$;
5. $|\mathcal{P}(A \times A)|$ ha cardinalità $2^{|A \times A|} = 2^9$.

Osservazione sul punto 3.: dovendo determinare la cardinalità di $A \cup \mathcal{P}(A)$, bisogna distinguere A come insieme, che ha cardinalità $|A| = 3$, da A come elemento di $\mathcal{P}(A)$. L'*insieme* A ha intersezione vuota con $\mathcal{P}(A)$, per cui $|A \cup \mathcal{P}(A)| = |A| + |\mathcal{P}(A)| = 3 + 8 = 11$.

3. *Enunciare il Teorema di Lagrange per un gruppo abeliano finito $(G, \cdot)$ di n elementi. Determinare un intero $m \in \mathbf{Z}_{\geq 1}$ tale che $\overline{x}^m \equiv \overline{1}$, per ogni $\overline{x} \in \mathbf{Z}_{200}^*$.*

Sol.: Teorema di Lagrange: *Sia $(G, \circ)$ un gruppo abeliano finito con n elementi. Allora per ogni $g \in G$, vale $g^n = e$, dove $g^n = \underbrace{g \circ g \circ \ldots \circ g}_{n \text{ volte}}$ ed e indica l'elemento neutro di G.*

Vedi le note!!!

Nel caso del gruppo $\mathbf{Z}_{200}^*$, che ha cardinalità $\varphi(200)$, il teorema dice che per ogni $\overline{x} \in \mathbf{Z}_{200}^*$ vale $\overline{x}^{\varphi(200)} = \overline{1}$. Dunque $\varphi(200) = \varphi(2^3 \cdot 5^2) = \varphi(2^3)\varphi(5^2) = (2^3 - 2^2)(5^2 - 5) = 4 \cdot 20 = 80$ è un intero che soddisfa le condizioni richieste.
Notare che tutti i multipli interi di 80 hanno la stessa proprietà.

4. *Determinare i seguenti resti (giustificando i vari passaggi)*

$$19^{145} \bmod 13, \qquad (-12)^{36} \cdot 50^{19} \bmod 7.$$

Sol.: Abbiamo innanzitutto che

$$19 \equiv 6 \bmod 13, \qquad -12 \equiv 2 \bmod 7, \qquad 50 \equiv 1 \bmod 7.$$

Inoltre $\varphi(13) = 12$ e per il Piccolo Teorema di Fermat (ossia il teorema di Lagrange applicato al gruppo $\mathbf{Z}_p^*$, con p primo) vale

$$x^{12} \equiv 1 \bmod 13, \quad \forall x \in \mathbf{Z}, \text{ per cui } \gcd(x, 13) = 1.$$

Segue che *modulo 13*

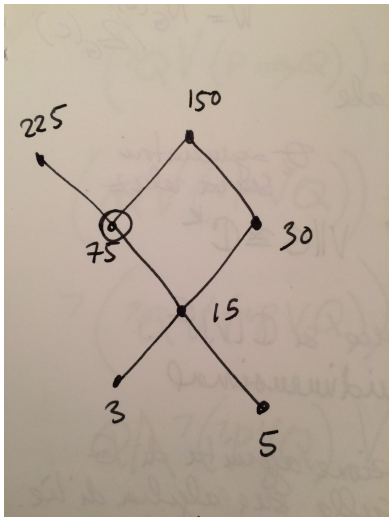
$$19^{145} \equiv 6^{145} \equiv 6^{144+1} \equiv (6^{12})^{12}6 \equiv 1 \cdot 6 \equiv 6.$$

Similmente abbiamo $\varphi(7) = 6$ e *modulo 7*

$$(-12)^{36} \cdot 50^{19} \equiv 2^{36} \cdot 1^{19} \equiv 2^{6 \cdot 6} \cdot 1 \equiv (2^6)^6 \equiv 1.$$

5. *Sia dato l'insieme* $X = \{3, 5, 15, 30, 75, 150, 225\}$ *con l'ordinamento parziale* " $\leq$ " *dato dalla divisibilità:*
   dati $m, n \in X$, m " $\leq$ " n *se* m *divide* n.
   (a) *Disegnare il diagramma di Hasse di* $(X, \leq)$.
   (b) *Determinare elementi minimali e massimali, ed eventuali massimo e minimo di* X.
   (c) *Determinare l'insieme dei maggioranti e l'insieme dei minoranti di* $A = \{75\}$.

Sol.: (a) Il diagramma di Hasse di X è raffigurato qui sotto:



(b) Elementi massimali: 225 e 150;

elementi minimali: 3 e 5;
Non ci sono né massimo né minimo in X.
(vedi definizioni sulle dispense!)

(c) I maggioranti di $\{75\}$ sono tutti gli elementi $x \in X$ tali che $75 \text{“} < \text{”} x$:

$$magg(\{75\}) = \{75, 225, 150\}.$$

I minoranti di $\{75\}$ sono tutti gli elementi $x \in X$ tali che $x \text{“} < \text{”} 75$:

$$minor(\{75\}) = \{75, 15, 3, 5\}.$$

6. *Sia $\mathcal{A}$ l'enunciato dato da $(\neg Q \vee (P \Rightarrow Q)) \Rightarrow \neg P$.*
   (a) Scrivere $\mathcal{A}$ come "somma di prodotti" (la negazione può stare solo di fronte ad una variabile).
   (a) Determinare se $\mathcal{A}$ è o meno una tautologia.

Sol.: (a) L'implicazione $\Rightarrow$ può essere espressa in termini di $\neg$ e $\vee$, ossia $P \Rightarrow Q$ è logicamente equivalente a $\neg P \vee Q$.
Quindi $(\neg Q \vee (P \Rightarrow Q)) \Rightarrow \neg P$ è logicamente equivalente a

$$\neg(\neg Q \vee (\neg P \vee Q)) \vee \neg P$$

$$Q \wedge \neg(\neg P \vee Q) \vee \neg P$$

$$Q \wedge P \wedge \neg Q \vee \neg P$$

$$Q \wedge \neg Q \wedge P \vee \neg P$$

(b) Verifichiamo che $\mathcal{A}$ non è una tautologia:
$Q \wedge \neg Q$ è sempre falsa;
$Q \wedge \neg Q \wedge P$ è sempre falsa;
$Q \wedge \neg Q \wedge P \vee \neg P$ è falsa se $\neg P$ è falsa, ossia P è vera, ed è vera se $\neg P$ è vera, ossia P è falsa.