ALGEBRA E LOGICA (Geatti) — 1° appello — Roma, 8 febbraio 2012, ore 14-16.

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 della congruenza* $8x \equiv 2 \bmod 14$. *Determinare tutte le soluzioni comprese nell'intervallo* $[0, 50]$.

Sol. Poiché $mcd(8, 14) = 2$ e $2|2$, la congruenza ha soluzioni intere. Inoltre è equivalente alla congruenza

$$4x \equiv 1 \bmod 7. \qquad (*)$$

Poiché $\mathrm{mcd}(4, 7) = 1$, la soluzione genale della (*) è data dagli interi della forma

$$x = x_0 + 7k, \quad k \in \mathbb{Z},$$

dove x_0 è una soluzione particolare. Costruiamo una soluzione particolare della (*) a partire da una soluzione particolare dell'equazione diofantea $4x - 7y = 1$. Ad esempio $(2, 1)$. Conclusione: la soluzione generale della (*) è data dagli interi $x = 2 + 7k$, al variare di $k \in \mathbb{Z}$.

Le soluzioni comprese nell'intervallo $[0, 50]$ sono

$$\{2,\ 9,\ 16,\ 23,\ 30,\ 37,\ 44\},$$

e corrispondono rispettivamente a $k = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6$.

2. *Sull'insieme* $\mathbb{Z}$ *sia data la seguente relazione: a R b se* $a^2 \equiv b^2 \bmod 5$.
   (a) Dimostrare che R è una relazione di equivalenza.
   (b) Determinare le classi di equivalenza di $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ *rispetto ad R, elencandone gli elementi.*

Sol. (a) Il fatto che R sia una relazione di equivalenza segue direttamente dal fatto che la *congruenza modulo 5* lo è. Si dimostra allo stesso modo....

(b) Le classi di equivalenza di $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ rispetto ad R contengono gli elementi di X i cui quadrati sono uguali modulo 5. Calcolando modulo 5, troviamo

$$1^2 \equiv 4^2 \equiv 6^2 \equiv 9^2 \equiv 11^2 \equiv 1, \qquad 2^2 \equiv 3^2 \equiv 7^2 \equiv 8^2 \equiv 4, \qquad 5^2 \equiv 10^2 \equiv 0.$$

Ne segue che le classi di equivalenza sono

$$\{1, 4, 6, 9, 11\}, \qquad \{2, 3, 7, 8\}, \qquad \{5, 10\}.$$

Notare che determinano una partizione di X, cioè X è unione disgiunta delle classi di equivalenza rispetto ad R.

3. *Calcolare il resto della divisione per 11 di* $13^{165} + 23^{5000} \cdot 15^{100002}$, *spiegando bene quali proprietà dei resti si sono usate.*

Sol. Per il calcolo usiamo i seguenti fatti: il resto di una somma è dato dalla somma dei resti, il resto di un prodotto è dato dal prodotto dei resti. Usiamo inoltre il Piccolo Teorema di Fermat: nel nostro caso dice che $x^{10} \equiv 1 \bmod 11$, se $mcd(x, 11) = 1$.

Calcolando modulo 11, troviamo

$$13^{165} + 23^{5000} \cdot 15^{100002} \equiv 2^{165} + 1^{5000} \cdot 4^{100002} \equiv$$

$$2^5 + 1 \cdot 4^2 \equiv 10 + 16 \equiv 4 \bmod 11.$$

4. Sia $\mathbb{Z}_{14}^*$ l'insieme delle classi resto modulo 14 che ammettono inverso moltiplicativo.
   (b) Elencare gli elementi di $\mathbb{Z}_{14}^*$, indicando l'inverso moltiplicativo di ogni classe.
   (b) Enunciare il Teorema di Lagrange per il gruppo $\mathbb{Z}_{14}^*$.
   (c) Esibire una classe $\bar{x} \in \mathbb{Z}_{14}$ per cui non vale l'enunciato della parte (b), giustificando la risposta.

Sol. Gli elementi di $\mathbb{Z}_{14}^*$ sono le classi resto $\bar{x} \in \mathbb{Z}_{14}$ con $\mathrm{mcd}(x, 14) = 1$:

$$\mathbb{Z}_{14}^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{9}, \overline{11}, \overline{13}\}.$$

Si verifica facilmente che

$$\bar{1}^{-1} = \bar{1}, \quad \bar{3}^{-1} = \bar{5}, \quad \bar{5}^{-1} = \bar{3}, \quad \bar{9}^{-1} = \overline{11}, \quad \overline{11}^{-1} = \bar{9}, \quad \overline{13}^{-1} = \overline{13}.$$

Per esempio $\bar{3} \cdot \bar{5} = \overline{15} = \bar{1}, \quad \bar{9} \cdot \overline{11} = \overline{99} = \bar{1}, \quad$ etc....
(b) Il Teorema di Lagrange per il gruppo $\mathbb{Z}_{14}^*$ dice:

$$\bar{x}^{\varphi(14)} = \bar{1}, \quad \forall \bar{x} \in \mathbb{Z}_{14}^*,$$

cioè

$$x^{\varphi(14)} = x^6 \equiv 1 \bmod 14, \quad \text{se } \ mcd(x, 14) = 1.$$

(c) L'enunciato in (b) non vale per le classi $\bar{x} \in \mathbb{Z}_{14}$ che non appartengono a $\mathbb{Z}_{14}^*$. Ad esempio $\bar{x} = \bar{2}$. Infatti

$$2^6 = 64 \not\equiv 1 \bmod 14.$$

5. Sia $X = \{x, y, z, t\}$ un insieme e sia $\mathcal{P}(X)$ l'insieme delle parti di X, ordinato rispetto alla relazione di inclusione: A"$\leq$"B se $A \subset B$. Sia S un sottoinsieme di $\mathcal{P}(X)$.
   (a) Richiamare la definizione di insieme dei maggioranti $magg(S)$ e quella di insieme dei minoranti $min(S)$ di S.
   (b) Determinare $magg(S)$ e $min(S)$, quando $S = \{\{x, y\}, \{y\}\} \subset \mathcal{P}(X)$ (elencarne gli elementi).
   (c) Determinare se S ammette estremo superiore, estremo inferiore, massimo o minimo (spiegare).

Sol. (a) $magg(S) = \{A \in \mathcal{P}(X) \mid s \subset A, \ \forall s \in S\} \quad$ e $\quad min(S) = \{B \in \mathcal{P}(X) \mid B \subset s, \ \forall s \in S\}$;
(b) $magg(S) = \{A \in \mathcal{P}(X) \mid \begin{cases} \{y\} \subset A \\ \{x, y\} \subset A \end{cases}\} = \{\{x, y\}, \{x, y, z\}, \{x, y, t\}, X\}$

$$min(S) = \{B \in \mathcal{P}(X) \mid \begin{cases} B \subset \{y\} \\ B \subset \{x, y\} \end{cases}\} = \{\emptyset, \{y\}\}.$$

(c) Abbiamo che $sup(S) = max(S) = \{x, y\} \quad$ e $\quad inf(S) = min(S) = \{y\}$.

6. Determinare la successione $\{a_n\}_{n \in \mathbb{N}}$ che soddisfa l'equazione ricorsiva $\begin{cases} a_n - a_{n-2} = 3^n \\ a_0 = 0, \ a_1 = 2. \end{cases}$

Sol. Le radici del polinomio $\lambda^2 - 1$, associato all'equazione lineare omogenea a coefficienti costanti

$$a_n - a_{n-2} = 0, \qquad (**)$$

sono ± 1. Ne segue che la soluzione generale dell'equazione è data dalle successioni di termine generale

$$S_n = A + B(-1)^n, \quad A, B \in \mathbb{R};$$

una soluzione particolare dell'equazione completa va ricercata della forma $\xi_n = c3^n$. Sostituendo ξ_n nell'equazione e imponendo che sia soluzione, si trova $c = 9/8$.
La soluzione generale dell'equazione completa è dunque

$$T_n = A + B(-1)^n + \frac{9}{8}3^n, \quad A, B \in \mathbb{R}.$$

Le condizioni iniziali

$$\begin{cases} A + B + \frac{9}{8} = 0 \\ A - B + \frac{9}{8} \cdot 3 = 2 \end{cases}$$

determinano univocamente A e B.