Algebra e Logica 2015 (Geatti-Iannuzzi) 3° appello bis Roma, 11 luglio 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 della congruenza* $8x \equiv 2 \bmod 18$. *Determinare tutte le soluzioni comprese nell'intervallo* $[0, 30]$.

Sol. Poiché $mcd(8, 18) = 2$ e $2|2$, la congruenza ha soluzioni intere. Inoltre è equivalente alla congruenza

$$4x \equiv 1 \bmod 9. \qquad (*)$$

Un intero x è soluzione della (*) se e solo se esiste un intero y tale che

$$4x - 9y = 1. \qquad (**)$$

Poiché $mcd(4, 9) = 1$, tutte e sole le soluzioni intere della equazione diofantea (**) sono date dalle coppie

$$(x, y) = (-2, -1) + k(9, 4) = (-2 + 9k, -1 + 4k), \text{al variare di } k \in \mathbf{Z}.$$

Ne segue che tutte e sole le soluzioni intere della congruenza (*) sono date da

$$x = -2 + 9k, \quad \text{al variare di } k \in \mathbf{Z}.$$

Le soluzioni comprese nell'intervallo $[0, 30]$ sono

$$\{7, 16, 25\},$$

e corrispondono rispettivamente a $k = 1,\ 2,\ 3$.

2. *Determinare la cardinalità dei seguenti insiemi, motivando le risposte:*

$$(a) \quad X = \{a, b, \{b\}, \{b, c\}, \{\{c\}\}\}, \qquad (b) \quad \mathcal{P}(\{a, b\}), \qquad (c) \quad Y = \{x \in \mathbf{Z} \mid -3 \leq x\} \cap \{x \in \mathbf{Z} \mid x < 1\},$$

$$(d) \quad B = \{x \in \mathbf{Z} \mid x \equiv 2 \bmod 5\}, \qquad (e) \quad \mathbf{N} \setminus \{1, 2, 3\}.$$

Sol.: (a) Gli elementi di X sono elencati, separati dalla virgola. Dunque $|X| = 5$.
(b) $|\mathcal{P}(\{a, b\})| = 2^2 = 4$.
(c) $Y = \{-3, -2, -1, 0\}$, per cui $|Y| = 4$.
(d) $B = \{x \in \mathbf{Z} \mid x = 2 + 5k,\ k \in \mathbf{Z}\}$. Definiamo

$$f\colon \mathbf{Z} \to B, \quad f(k) = 2 + 5k.$$

Si verifica facimente che f è una funzione biiettiva: è suriettiva per costruzione ed è iniettiva perche' $f(k) = 2 + 5k = f(h) = 2 + 5h$ se e solo se $k = h$. Dunque B ha la stessa cardinalità di $\mathbf{Z}$ e di $\mathbf{N}$, cioè quella del numerabile.
(e) la cardinalità di $\mathbf{N} \setminus \{1, 2, 3\}$ è uguale a quella di $\mathbf{N}$, cioè quella del numerabile. Infatti la mappa $f\colon \mathbf{N} \to \mathbf{N} \setminus \{1, 2, 3\}, \quad f(n) = n + 3$ è biettiva.

3. *Determinare quanti elementi ha* Z_{250}^*, *l'insieme delle classi resto modulo 250 che ammettono inverso moltiplicativo. Calcolare, se esistono, l'inverso di* 81 *e l'inverso di* 15 *in* Z_{250}^*.

Sol.: Poiché $250 = 2 \cdot 5^3$, la cardinalità di Z^*_{250} è uguale $\varphi(250) = \varphi(2)\varphi(5^3) = 5^3 - 5^2 = 125 - 25 = 100$, dove φ è la funzione di Eulero il cui valore in $n \in \mathbf{N}$ è per definizione la cardinalità di Z^*_n.

Un elemento $\bar{a} \in \mathbf{Z}_{250}$ ammette inverso moltilicativo se e solo se $mcd(a, 250) = 1$. Dunque $\overline{15}$ non ammette inverso moltiplicativo, mentre $\overline{81}$ ammette inverso moltiplicativo. Per trovarlo si usa l'algoritmo di euclide esteso. Abbiamo

$$250 = 3 \cdot 81 + 7, \quad 81 = 11 \cdot 7 + 4, \quad 7 = 1 \cdot 4 + 3, \quad 4 = 1 \cdot 3 + 1,$$

da cui

$$1 \cdot 250 + 0 \cdot 81 = 250$$

$$0 \cdot 250 + 1 \cdot 81 = 81$$

$$1 \cdot 250 + (-3) \cdot 81 = 7$$

$$(-1) \cdot 250 + (34) \cdot 81 = 4$$

$$(12) \cdot 250 + (-37) \cdot 81 = 3$$

$$(-23) \cdot 250 + (71) \cdot 81 = 1.$$

Dunque $\overline{81}^{-1} = \overline{71}$ in Z^*_{250}.

4. *Determinare l'ultima cifra di* 3^{1024}*, motivando i vari passaggi.*

Sol.: Determinare l'ultima cifra di 3^{1024} equivale a calcolarne la classe resto modulo 10. Osserviamo che $mcd(3, 10) = 1$, per cui $3 \in \mathbf{Z}^*_{10}$. Possiamo quindi applicare il Teorema di Lagrange al gruppo $(\mathbf{Z}^*_{10}, \cdot)$, che ha cardinalità $\varphi(10) = 4$, ed abbiamo che

$$3^4 \equiv 1 \bmod 10.$$

Ne segue che

$$3^{1024} = 3^{4 \cdot 256} = (3^4)^{256} \equiv 1 \bmod 10,$$

e la cifra cercata è uguale a 1.

5. Determinare se le due affermazioni sono vere o false sul dominio $\mathbf{Q} \setminus \{0\}$, ossia quando $x, y \in \mathbf{Q} \setminus \{0\}$, spiegando bene le risposte:

$$\forall x(\exists y \ xy = 1), \qquad \exists x(\forall y \ \ xy = 1).$$

Sol.: La prima affermazione è vera: dice che ogni $x \in \mathbf{Q} \setminus \{0\}$ ammette un reciproco in $\in \mathbf{Q} \setminus \{0\}$. Basta prendere $y = 1/x$: se $x \in \mathbf{Q} \setminus \{0\}$, anche $y = 1/x \in \mathbf{Q} \setminus \{0\}$.

La seconda affermazione è falsa: nessun $x \in \mathbf{Q} \setminus \{0\}$, moltiplicato per tutti gli $y \in \mathbf{Q} \setminus \{0\}$ dà sempre 1. Il reciproco è unico: infatti $xy = xy' = 1$ implica $y = y'$.

6. *In un'algebra di Boole* $(A, +, \cdot, ')$*, siano date le espressioni*

$$E: \quad xy'z + y'z' + xy'z', \qquad F: \quad xyz + x'y + xz.$$

   (a) determinare se E *ed* F *sono equivalenti;*
   (b) scrivere E *come somma di implicanti primi;*
   (c) determinare una forma minimale di E*.*

Sol.: (a) & (b) Portiamo entrambe le espressioni nella forma *somma di tutti gli implicanti primi.* Poiché tale forma è unica, ci dirà se E ed F sono o meno equivalenti, ed avremo risposto anche alla domanda (b). Applicando le proprietà delle operazioni di $(A, +, \cdot, ')$ troviamo

$$E: \quad xy'z + y'z' + xy'z' \ = \ xy'(z + z') + y'z' \ = \ xy' + y'z'.$$

Poiché il metodo del consenso non ha passi non banali, quella che abbiamo trovato è la somma di tutti gli implicanti primi di E.
Similmente

$$F: \quad xyz + x'y + xz \quad = \quad xz(y+1) + x'y \;=\; xz + x'y \;=\; xz + x'y + zy,$$

dove l'ultima uguaglianza è stata ottenuta sommando zy, che è il consenso tra xz e $x'y$. Poiché il metodo del consenso non ha passi non banali, quella che abbiamo trovato è la somma di tutti gli implicanti primi di F.
Ne segue che E ed F non sono equivalenti.
(c) Per determinare una forma minimale di E, completiamo $xy' + y'z'$:

$$xy' + y'z' = (xy'z + xy'z') + (xy'z' + x'y'z').$$

Poiché i due addendi sono distinti, nessuno dei due può essere eliminato. Dunque $xy' + y'z'$ è una forma minimale di E.