Matematica Discreta 2014 Informatica (Geatti) 1^o appello Roma 5 febbraio 2015, 10:00–12:30.

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 4,5 punti.

1. *Determinare tutte le soluzioni intere della congruenza* $4x \equiv 2 \bmod 101$. *Determinare tutte le soluzioni comprese nell'intervallo* $[0, 500]$.

Sol.: Un intero $x \in \mathbf{Z}$ è soluzione della congruenza se e solo se esiste $k \in \mathbf{Z}$ tale che $4x - 101k = 2$. Le soluzioni dell'equazione diofantea $4x - 101k = 2$ sono date dalle coppie di interi

$$(x, k) = (x_0, k_0) + Sol(2x - 101k = 0) = (-50, -2) + (101M, 2M), \quad \text{al variare di } M \in \mathbf{Z}.$$

Dunque le soluzioni della congruenza originaria sono date da

$$x = -50 + 101M = 51 + 101M, \quad \text{al variare di } M \in \mathbf{Z}.$$

Le soluzioni comprese nell'intervallo $[0, 500]$ sono $51,\ 152,\ 253,\ 354,\ 455$, e corrispondono rispettivamente ai valori di $M = 0, 1, 2, 3, 4$.

2. *Sia* $\mathbf{Z}^*_{100}$ *l'insieme delle classi resto modulo* 100 *che ammettono inverso moltiplicativo.*
   (a) Verificare che $\overline{33} \in \mathbf{Z}^*_{100}$.
   (b) Determinare un intero m *tale che* $\overline{m} = \overline{33}^{-1} \in \mathbf{Z}^*_{100}$.

Sol.: (a) Abbiamo che $\overline{33} \in \mathbf{Z}^*_{100}$ se e solo se $mcd(33, 100) = 1$. Effettivamente $mcd(33, 100) = 1$ (cf. algoritmo di Euclide, o semplicemente $33 = 3 * 11$ e $100 = 2^2 * 5^2$).
(b) L'intero cercato si ricava da una soluzione particolare dell'equazione diofantea

$$33x = 1 + 100k \quad \Leftrightarrow \quad 33x - 100k = 1. \tag{$*$}$$

È evidente che $(x_0, k_0) = (-3, -1)$ è una soluzione particolare dell'equazione (*) (altrimenti si ottiene dall'algoritmo di Euclide esteso), da cui $m = -3$ è l'intero cercato.
N.B.: è equivalente scegliere $m = 97$ o qualunque altro intero congruo a 97 modulo 100. Tutti definiscono la stessa classe $\overline{33}^{-1} = \overline{97} \in \mathbf{Z}^*_{100}$.

3. *Enunciare il teorema di Lagrange per un gruppo abeliano finito* $(G, \cdot)$ *di* n *elementi. Determinare* $m \in \mathbf{Z}_{\geq 1}$ *tale* $\overline{x}^m \equiv \overline{1}$*, per ogni* $\overline{x} \in \mathbf{Z}^*_{100}$.

Sol.: Per il Teorema di Lagrange: vedi dispense.
L'intero cercato è $m = \varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2 - 2)(5^2 - 5) = 40$. Infatti $|\mathbf{Z}^*_{100}| = \varphi(100) = 40$ e per il Teorema di Lagrange

$$\overline{x}^{40} \equiv \overline{1}, \quad \text{in } \mathbf{Z}^*_{100}.$$

Notare che $m = 40$ è il più piccolo intero con la proprietà richiesta. Ogni multiplo intero di 40 funziona.

4. *Determinare tutte le soluzioni dell'equazione ricorsiva* $F_n - 2F_{n-1} = 2^n, \quad n \geq 1$.

Sol.: In questo caso non abbiamo condizioni iniziali. Quindi determiniamo la famiglia (infinita) di tutte le funzioni ricorsive il cui termine generale soddisfa l'equazione data:

$$S_n = \xi_n + Sol(F_n - 2F_{n-1} = 0).$$

Il polinomio associato all'equazione omogenea associata è $\lambda - 2$, con radice $\lambda = 2$. Dunque le soluzioni dell'equazione omogenea associata $F_n - 2F_{n-1} = 0$ sono

$$A2^n, \quad \text{al variare di } A \in \mathbf{R}.$$

Poiché 2 è già radice del polinomio associato di molteplicità $m = 1$, la soluzione particolare si cerca della forma

$$\xi_n = \alpha n 2^n,$$

con α una costante reale da determinarsi sostituendo $\xi_n = \alpha n 2^n$ nell'equazione di partenza :

$$\alpha n 2^n - 2\alpha(n-1)2^{n-1} = 2^n \quad \Leftrightarrow \quad \alpha = 1.$$

Conclusione: le soluzioni dell'equazione $F_n - 2F_{n-1} = 2^n$ sono

$$S_n = n2^n + A2^n, \quad \text{al variare di } A \in \mathbf{R}.$$

5. Siano dati $A = \{x, y, z, u\}$ e $B = \{1, 2, 3, 4\}$. Determinare la cardinalità dei seguenti insiemi:

$\{f : A \to B\}$, $\{f : A \to B \mid f(x) \neq f(y)\}$, $\{f : A \to B \mid \text{iniettive}\}$, $\{f : A \to B \mid f(x) = f(y) = 1\}$.

Sol.: (a) Per ognuno dei valori $f(x)$, $f(y)$, $f(z)$, $f(w)$ ci sono 4 scelte, e sono tutte indipendenti: dunque la cardinalità dell'insieme $\{f : A \to B\}$ risulta $4 \cdot 4 \cdot 4 \cdot 4 = 4^4$.

(b) Per $f(x)$ ci sono 4 scelte, per $f(y) \neq f(x)$ ce ne sono 3, per $f(z)$ ed $f(w)$ ce ne sono 4, e sono tutte indipendenti: dunque la cardinalità dell'insieme $\{f : A \to B \mid f(x) \neq f(y)\}$ risulta $4 \cdot 3 \cdot 4 \cdot 4 = 3 \cdot 4^3$.

(c) Per $f(x)$ ci sono 4 scelte, per $f(y)$, che deve essere $\neq f(x)$, ce ne sono 3, per $f(z)$, che deve essere diverso da $f(x)$ ed $f(y)$, ce ne sono 2, per $f(w)$, che deve essere diverso da $f(x)$, $f(y)$ ed $f(z)$, ce ne è una sola. Conclusione: la cardinalità dell'insieme $\{f : A \to B \mid \text{iniettive}\}$ risulta $4 \cdot 3 \cdot 2 \cdot 1$.

(d) Poiché $f(x) = f(y) = 1$, in questo caso ci sono solo 4 scelte per $f(z)$ e 4 scelte per $f(w)$, indipendenti una dall'altra. Dunque la cardinalità dell'insieme $\{f : A \to B \mid f(x) = f(y) = 1\}$ risulta $4 \cdot 4$.

6. *Siano A e B insiemi e sia $f\colon A \to B$ una funzione.*
   (a) Usando i quantificatori $\forall$ e $\exists$, esprimere "f è suriettiva".
   (b) Determinare se $f\colon \mathbf{Z} \to \mathbf{Z}$, data da $f(n) = 2n - 3$ è suriettiva.

Sol.: (a) Per definizione la funzione $f\colon A \to B$ è suriettiva se:

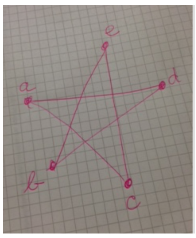
$$\forall b \in B \quad \exists a \in A : \quad f(a) = b.$$

(b) Al variare di $n \in \mathbf{Z}$, abbiamo che $f(n) = 2n - 3$ è un intero dispari. Dunque f non è suriettiva. Usando la definizione del punto precedente, abbiamo che dato $a \in \mathbf{Z}$, esiste $n \in \mathbf{Z}$ tale che

$$2n - 3 = a \quad \Leftrightarrow \quad n = (a+3)/2 \quad \Leftrightarrow \quad a \text{ è dispari.}$$

7. *Richiamare la caratterizzazione dei grafi che ammettono un circuito o un cammino euleriano. Determinare se il grafo qui sotto ammette un circuito o un cammino euleriano. Se si', indicarlo elencando i vertici in ordine di percorrenza.*

Sol.: Per *la caratterizzazione..etc..*: vedi testo.



In base a tale caratterizzazione, il grafo ammette un circuito euleriano: tutti vertici sono di grado 2. Un circuito euleriano è dato ad esempio da $a \to c \to e \to b \to d \to a$.