Matematica Discreta 2014 Informatica (Geatti) 2° appello Roma 23 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 del sistema di congruenze* $\begin{cases} x \equiv 2 \bmod 4 \\ 3x \equiv 2 \bmod 10. \end{cases}$

Sol.: Le congruenze hanno singolarmente soluzioni intere: per la prima è evidente, per la seconda abbiamo che $mcd(3, 10) = 1$ & 1 divide 2. Le soluzioni della prima congruenza sono gli interi della forma

$$x = 2 + 4k, \quad \text{al variare di } k \in \mathbf{Z}. \qquad (*)$$

Sostituendole nella seconda, troviamo

$$3(2 + 4k) = 2 + 10h \quad \Leftrightarrow \quad 12k - 10h = -4 \quad \Leftrightarrow \quad 6k - 5h = -2, \quad k, h \in \mathbf{Z}. \qquad (**)$$

Le soluzioni dell'equazione diofantea (**) sono le coppie di interi

$$(k, h) = (-2, -2) + M(5, 6) = (-2 + 5M, -2 + 6M), \quad \text{al variare di } M \in \mathbf{Z}.$$

Il significato delle soluzioni dell'equazione diofantea (**) è questo: gli interi $k = -2 + 5M$, $M \in \mathbf{Z}$, sostituiti nella equazione (*), parametrizzano le soluzioni della prima congruenza che sono anche soluzioni della seconda.
Conclusione: le soluzioni del sistema di partenza sono gli interi

$$x = 2 + 4(-2 + 5M) = 2 - 8 + 20M = -6 + 20M = 14 + 20M, \quad \text{al variare di } M \in \mathbf{Z}.$$

2. *Calcolare* $7^{12^6} + 12^{6^7} \bmod 13$*, citando i risultati usati nello svolgimento.*

Sol.: Poiché 13 è primo, per Piccolo Teorema di Fermat $a^{12} \equiv 1 \bmod 13$, per ogni intero a con $mcd(a, 13) = 1$.
Abbiamo $mcd(7, 13) = 1$. Inoltre 12^6 è un multiplo intero di 12. Ne segue che

$$7^{12^6} \equiv (7^{12})^{12^5} \equiv 1 \bmod 13.$$

Poiché $12 \equiv -1 \bmod 13$ e 6^7 è pari, $12^{6^7} \equiv (-1)^{6^7} \equiv 1 \bmod 13$.
Conclusione:

$$7^{12^6} + 12^{6^7} \equiv 1 + 1 = 2 \bmod 13.$$

3 *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 $N = 85$ e $D = 13$.
   (b) Il signor Rossi riceve il messaggio criptato $m = 19$. Che cosa calcola per decriptarlo?
   (c) Che cosa si calcola per criptare il messaggio $m = 23$ da inviare al signor Rossi?

Sol.: (a) Abbiamo $N = 85 = 5 \cdot 17$, cioè $N = p \cdot q$ con $p = 5$ e $q = 17$. La chiave E è per definizione

$$E = D^{-1} \quad \bmod (p-1)(q-1), \quad \text{cioè} \quad E = 13^{-1} \bmod 64.$$

Notare che E esiste perché $mcd(13, 64) = 1$.
Cerchiamo $x \in \mathbf{Z}$ tale che

$$13x \equiv 1 \bmod 64 \quad \Leftrightarrow \quad \exists y \in \mathbf{Z} \quad 13x - 64y = 1.$$

Una soluzione particolare dell'equazione diofantea $13x - 64y = 1$ è data da $(5, 1)$ (a occhio oppure con 2 passi dell'algoritmo di Euclide esteso). Dunque $E = 5$ è la chiave cercata.

(b) Per decriptare il messaggio ricevuto, Rossi calcola $m^D \bmod N$, cioè $19^{13} \bmod 85$.

(c) Per criptare il messaggio $m = 23$ da inviare al signor Rossi, calcoliamo $m^E \bmod N$, cioè $23^5 \bmod 85$.

4. *(a) Risolvere l'equazione ricorsiva* $\begin{cases} F_n - 10F_{n-1} + 25F_{n-2} = 0, & n \geq 2, \\ F_0 = 1, \quad F_1 = 0. \end{cases}$

   (b) Calcolare F_{100} ed F_{101}.

Sol.: (a) L'equazione è omogenea di grado 2, a coefficienti costanti. Il polinomio associato è $\lambda^2 - 10\lambda + 25 = (\lambda - 5)^2$, con radici reali e coincidenti $\lambda_1 = \lambda_2 = 5$. Ne segue che la famiglia delle soluzioni dell'equazione, prima di imporre le condizioni iniziali, è data da

$$S_n = A5^n + Bn5^n, \quad \text{al variare di } A,\ B \in \mathbf{R}.$$

Dalle condizioni

$$\begin{cases} S_0 = A \cdot 5^0 + B \cdot 0 \cdot 5^0 = A = 1 \\ S_1 = A \cdot 5^1 + B \cdot 1 \cdot 5^1 = 5A + 5B = 0, \end{cases}$$

ricaviamo $A = 1$ e $B = -1$.

Conclusione:

la soluzione dell'equazione $\begin{cases} F_n - 10F_{n-1} + 25F_{n-2} = 0, & n \geq 2, \\ F_0 = 1, \quad F_1 = 0 \end{cases}$ è data da

$$\xi_n = 5^n - n5^n.$$

(b) $F_{100} = 5^{100} - 100 \cdot 5^{100} = -99 \cdot 5^{100}$; $\qquad F_{101} = 5^{101} - 101 \cdot 5^{101} = -100 \cdot 5^{101}$.

5. *Determinare il numero delle stringhe ordinate di 4 cifre in $\{0, 1, \ldots, 9\}$, in ognuno dei seguenti casi:*
   (a) Iniziano o terminano con una cifra pari.
   (b) Hanno precisamente due cifre uguali a 9.
   (c) Contengono due volte la stessa cifra.

Sol.: (a) L'insieme cercato è $A \cup B$, dove

$$A = \{XYZW \mid Y, Z, W \in \{0, \ldots, 9\},\ X \in \{0, 2, 4, 6, 8\}\}$$

è l'insieme delle stringhe che iniziano con una cifra pari e

$$B = \{XYZW \mid X, Y, Z \in \{0, \ldots, 9\},\ W \in \{0, 2, 4, 6, 8\}\}$$

è l'insieme delle stringhe che terminano con una cifra pari.

Per il principio di inclusione-esclusione, la cardinalità di $A \cup B$ è data da

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Osserviamo che

$$A \cap B = \{XYZW \mid Y, Z \in \{0, \ldots, 9\},\ X, W \in \{0, 2, 4, 6, 8\}\}$$

è l'insieme delle stringhe che iniziano & terminano con una cifra pari. Abbiamo

$$|A| = 5 \cdot 10^3, \quad |B| = 5 \cdot 10^3, \quad |A \cap B| = 5^2 \cdot 10^2,$$

da cui $|A \cup B| = 5 \cdot 10^3 + 5 \cdot 10^3 - 5^2 \cdot 10^2 = 10^4 - 25 \cdot 10^2 = 7500$.

(b) Le due cifre uguali a 9 si possono disporre in sei modi (tanti quanti sono i sottoinsiemi di 2 elementi in un insieme di 4 elementi)

$$99XY, \quad 9X9Y, \quad 9XY9, \quad X99Y, \quad X9Y9, \quad XY99,$$

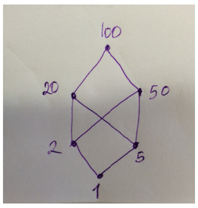
con $X, Y \in \{0, \dots, 8\}$. In totale ci sono $6 \cdot 9^2$ stringhe che hanno esattamente due cifre uguali a 9.
(c) Le due cifre uguali, che questa volta possono variare da 0 a 9, si possono disporre in sei modi:

$$WWXY, \quad WXWY, \quad WXYW, \quad XWWY, \quad XWYW, \quad XYWW,$$

con $W \in \{0, \dots, 9\}$ e $X, Y \neq W$ & $X \neq Y$. In totale ci sono $10 \cdot 6 \cdot 9 \cdot 8$ stringhe che hanno esattamente due cifre uguali.

6. *Sia* $X = \{1, 2, 5, 20, 50, 100\}$ *con la relazione* R *data dalla divisibiltà:* kRn *se* k *divide* n.
   (a) Verificare che R *è una relazione di ordine su* X.
   (b) Disegnare il diagramma di Hasse di (X, R).
   (c) Determinare se (X, R) *è o meno un reticolo.*

Sol.: (a) La relazione R è una relazione d'ordine sull'insieme dei numeri naturali $\mathbf{N}$, e dunque anche su $X \subset \mathbf{N}$.
• R è riflessiva, cioè $xRx, \quad \forall x \in X$: infatti $x = 1 \cdot x$, cioè x divide x;
• R è antisimmetrica, cioè $\begin{cases} xRy \\ yRx \end{cases} \Rightarrow x = y$: infatti se x divide y, ossia esiste $k \in \mathbf{N}$ tale che $y = kx$, e y divide x, ossia esiste $h \in \mathbf{N}$ tale che $x = hy$, allora vale $y = kx = khy$. Questo è possibile se e solo se $k = h = 1$, cioè $x = y$.
• R è transitiva, cioè $\begin{cases} xRy \\ yRz \end{cases} \Rightarrow x = z$: infatti se x divide y, ossia esiste $k \in \mathbf{N}$ tale che $y = kx$, e y divide z, ossia esiste $h \in \mathbf{N}$ tale che $z = hy$, allora vale $z = hy = hkx$, cioè x divide z.
(b) Il diagranmma di Hasse di (X, R) è dato da



(c) L'insieme ordinato (X, R) ammette massimo e minimo, dati rispettivamente da 100 e 1. Di conseguenza, per ogni coppia di elementi $x, y \in X$ l'insieme dei maggioranti

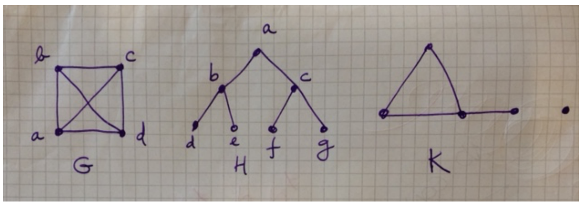
$$magg(x, y) = \{z \in X \mid xRz \ \& \ yRz\}$$

e quello dei minoranti

$$minor(x, y) = \{s \in X \mid sRx \ \& \ sRy\}$$

sono non vuoti. In particolare esistono $sup(x, y)$ (il minimo dei maggioranti) ed $inf(x, y)$ (il massimo dei minoranti) di x, y in X. Questo dice precisamente che X è un reticolo (vedi dispense).

7. *(a) Richiamare la definizione di numero cromatico di un grafo.*
   (b) Calcolare il numero cromatico dei grafi G *ed* H.
   (c) Calcolare il polinomio cromatico del grafo K.



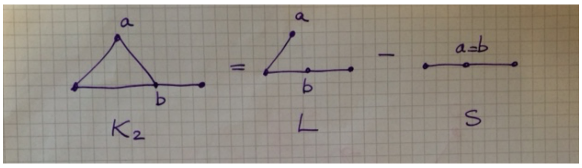
Sol.: (a) Vedi testi.

(b) Il grafo G è un grafo completo con 4 vertici. Il numero cromatico di G è $\chi(G) = 4$: un colore per il primo vertice a, due colori diversi fra loro e dal colore di a per i vertici b e d, ed un quarto colore per il vertice c. Il grafo H è un albero. Il numero cromatico di H è $\chi(H) = 2$: un colore per il primo vertice a, un colore diverso per i vertici b e c, e poi il colore usato per a può essere riusato per i vertici d, e, f, g, che non sono adiacenti ad a.

(c) Il grafo K è unione disgiunta di due componenti connesse $K = K_1 \cup K_2$, dove K_1 è un singolo vertice e K_2 è il resto. Il polinomio cromatico di K è dato da

$$p_K(\lambda) = p_{K_1}(\lambda) \cdot p_{K_2}(\lambda).$$

Per K_1 abbiamo $p_{K_1}(\lambda) = \lambda$. Per calcolare $p_{K_2}(\lambda)$ usiamo il teorema di cancellazione-contrazione:



da cui $p_{K_2}(\lambda) = p_L(\lambda) - p_S(\lambda) = \lambda(\lambda-1)^3 - \lambda(\lambda-1)^2$, usandoi il fatto che il polinomio cromatico di un albero con n vertici è dato da $\lambda(\lambda-1)^{n-1}$. Conclusione:

$$p_K(\lambda) = p_{K_1}(\lambda) \cdot p_{K_2}(\lambda) = \lambda(\lambda(\lambda-1)^3 - \lambda(\lambda-1)^2) = \lambda^2(\lambda-1)^2(\lambda-2).$$