Algebra e Logica 2015 (Geatti-Iannuzzi) 4° appello Roma, 15 settembre 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. *Siano dati i sistemi di congruenze* $\begin{cases} x \equiv 1 \mod 2 \\ 7x \equiv 3 \mod 4 \end{cases}$ *e* $\begin{cases} 2x \equiv 5 \mod 6 \\ x \equiv 3 \mod 4. \end{cases}$
   (i) Determinare quale dei due ha soluzioni intere.
   (ii) Determinare tutte le soluzioni intere di tale sistema.

Sol.: Il secondo sistema non ammette soluzioni intere: gia' la prima congruenza non ne ha, visto che $mcd(2,6) = 2$ che non divide 5.

Primo sistema: dalla congruenza ricaviamo $x = 1 + 2k,\ k \in \mathbf{Z}$ e sostituendo nella seconda otteniamo

$$7(1+2k) = 3 + 4h \quad \Leftrightarrow \quad 14k - 4h = -4 \quad \Leftrightarrow \quad 7k - 2h = -2, \qquad k, h \in \mathbf{Z}.$$

Risolvendo questa equazione diofantea, troviamo $k = 2+2M,\ M \in \mathbf{Z}$. Risostituendo nella prima congruenza, troviamo le soluzioni del sistema

$$x = 5 + 4M, \quad M \in \mathbf{Z}.$$

2. *Siano dati gli insiemi* $X = \{x_1, \dots, x_5\}$ *ed* $Y = \{y_1, \dots, y_7\}$. *Calcolare la cardinalità dei seguenti insiemi, spiegando per esteso il ragionamento fatto:*

$$A = \{f\colon X \to Y \mid f(x_1) = y_1\}, \quad B = \{f\colon X \to Y \mid f(x_1) = f(x_2),\ f(x_2) \neq y_1\},$$

$$C = \{f\colon X \to Y \mid f(x_1) \neq f(x_2),\ f(x_3) = y_7,\ f(x_4) = y_6\}, \quad D = \{f\colon X \to Y \mid \text{iniettive}\}.$$

Sol.: $\#A = 7^4$:
ci sono 7 scelte per $f(x_2),\ f(x_3),\ f(x_4),\ f(x_5)$ e sono tutte indipendenti. per $f(x_1)$ c'e' una scelta sola: $f(x_1) = y_1$.

$\#B = 7^3 \cdot 6$:
ci sono 7 scelte per $f(x_3),\ f(x_4),\ f(x_5)$, 6 scelte per $f(x_2)$ e una scelta per $f(x_1)$, una volta fissato $f(x_2)$, e sone tutte indipendenti.

$\#C = 7^2 \cdot 6$:
ci sono 7 scelte per $f(x_2),\ f(x_5)$, una scelta per $f(x_3),\ f(x_4)$, 6 scelte per $f(x_1) \neq f(x_2)$, e sone tutte indipendenti.

$\#D = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3$:
ci sono 7 scelte per $f(x_1)$, 6 scelte per $f(x_2)$, 5 scelte per $f(x_3)$, 4 scelte per $f(x_4)$ e 3 scelte per $f(x_5)$, e sono tutte indipendenti.

3. *Enunciare il Teorema di Lagrange per un gruppo abeliano finito* $(G, \cdot)$ *di* n *elementi. Determinare* $m \in \mathbf{Z}_{\geq 1}$ *tale* $\overline{x}^m = \overline{1}$, *per ogni* $\overline{x} \in \mathbf{Z}_{150}^*$.

Sol.: Per l'enunciato...vedi dispense.
Dall'enunciato, si ha che $m = \phi(150) = \phi(2)\phi(3)\phi(5^2) = 1 \cdot 2 \cdot 20 = 40$ soddisfa la richiesta. Lo stesso vale per ogni multiplo intero di 40.

4. *Calcolare* $3^{10^{5^{10}}} + 10^{6^5} \mod 11$.

Sol.: $3 \in \mathbf{Z}_{11}^*$. Dunque, per il Piccolo Teorema di Fermat, $3^{10} \equiv 1 \bmod 11$ e in generale $3^{k\cdot 10} \equiv 1 \bmod 11$, per ogni $k \in \mathbf{Z}$. Poiché $10^{5^{10}}$ è un multiplo intero di 10, vale $3^{10^{5^{10}}} \equiv 1 \bmod 11$. Inoltre $10 \equiv -1 \bmod 11$. Poiché 6^5 è pari, vale $10^{6^5} \equiv 1 \bmod 11$.
Conclusione: $3^{10^{5^{10}}} + 10^{6^5} \equiv 2 \bmod 11$.

5. *Il signor Rossi desidera ricevere messaggi criptati e adotta il criptosistema RSA.*
   (a) *Preparare per il signor Rossi un kit di chiavi pubbliche N, E e chiave segreta D, con $N = 85$ e $D = 43$.*
   (b) *Il signor Rossi riceve il messaggio criptato $m = 11$. Che cosa calcola per decriptarlo?*
   (c) *Vogliamo inviare al signor Rossi il messaggio $m = 34$. Che cosa calcoliamo per criptarlo?*

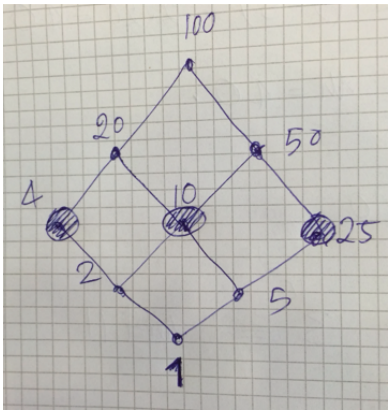
(ai punti (b) e (c) basta impostare il calcolo).

Sol.: (a) La chiave pubblica E è data da $E = D^{-1} \bmod (p-1)(q-1)$, dove p, q sono i fattori prmi di $N = pq$. Nel nostro caso, $N = 85 = 5 \cdot 17$, per cui $(p-1)(q-1) = 4 \cdot 16 = 64$ ed

$$E = 43^{-1} \bmod 64.$$

Notare che $mcd(43, 64) = 1$, per cui E esiste. Con due passaggi dell'algoritmo di Euclide esteso si trova $E = 3$ (prova: $3 \cdot 43 = 129 \equiv 1 \bmod 64$).
(b) Calcola $11^{43} \bmod 85$.
(c) Calcoliamo $34^3 \bmod 85$.

6. *Sia D_{100} l'insieme dei divisori di 100, con la relazione di ordine parziale dato dalla divisibilità.*
   (a) *Disegnare il diagramma di Hasse di D_{100}.*
   (b) *Dato il sottoinsieme $S = \{4, 10, 25\} \subset D_{100}$, determinare l'insieme dei maggioranti e l'insieme dei minoranti di S.*
   (c) *Determinare se gli elementi 4 e 10 ammettono o meno complemento. In caso affermativo, dire se tale complemento è unico.*



Sol.: (a) Diagramma di Hasse:

(b) 100 è l'unico elemento divisibile per $4, 10, 25$. Per cui $magg(S) = \{100\}$.
1 è l'unico elemento che divide $4, 10, 25$. Per cui $min(S) = \{1\}$.

(c) Il complemento di 4 è 25 ed è unico: infatti $mcm(4, 25) = 100$ e $mcd(4, 25) = 1$. Si può controllare che 25 è l'unico elemento di D_{100} con queste proprietà. Invece 10 non ammette complemento: non esiste $x \in D_{100}$ che soddisfa $mcm(x, 10) = 100$ e $mcd(x) = 1$.