Algebra e Logica 2015 (Geatti-Iannuzzi) 2° appello Roma, 19 febbraio 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 tutti gli interi X che soddisfano il sistema di congruenze*

$$\begin{cases} X \equiv 1 \mod 7 \\ X \equiv 3 \mod 13. \end{cases}$$

Sol.: È evidente che le congruenze del sistema hanno singolarmente soluzioni intere. Poiché $mcd(7, 13) = 1$, per il Teorema Cinese del Resto, anche il sistema ha soluzioni intere. Inoltre, le soluzioni sono della forma

$$X = X_0 + M(7 \cdot 13), \quad M \in \mathbf{Z},$$

dove X_0 è una soluzione particolare del sistema.

Le soluzioni della prima congruenza sono date dagli $X = 1 + 7k$, al variare di $k \in \mathbf{Z}$. Sostituendo questa relazione nella seconda congruenza troviamo

$$1 + 7k \equiv 3 \mod 13 \quad \Leftrightarrow \quad 1 + 7k = 3 + 13h, \quad k, h \in \mathbf{Z}$$

$$\Leftrightarrow \quad 7k + 13h = 2, \quad k, h \in \mathbf{Z}.$$

Troviamo facilmente che $7 \cdot 2 + 13 \cdot (-1) = 1$, quindi la soluzione generale dell'equazione $7k + 13h = 2$ risulta

$$\{(k, h) = (4, -2) + M(13, -7), \quad M \in \mathbf{Z}\}.$$

Da qui ricaviamo $k = 4 + 13M,\ M \in \mathbf{Z}$ che sostituita nella soluzione della prima congruenza ci dà la soluzione generale del sistema

$$\{X = 1 + 7k = 1 + 7(4 + 13M) = 29 + M(7 \cdot 13) = 29 + M91, \quad M \in \mathbf{Z}\}.$$

2. *Sia $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.*
   (a) Sia R la relazione su X data da xRy se $x+y$ è pari. Verificare che R è una relazione di equivalenza e determinare le classi di equivalenza corrispondenti.
   (b) Sia R la relazione su X data da xRy se $x + y$ è dispari. Determinare se R è o meno una relazione di equivalenza (giustificare).

Sol.: (a) La relazione R è:
riflessiva: per ogni $x \in X$ si ha che xRx: infatti $x + x$ è pari.
simmetrica: per ogni $x, y \in X$ si ha che xRy implica yRx: infatti se $x + y$ è pari, anche $y + x$ è pari.
transitiva: se xRy e yRz, allora anche xRz: osserviamo che $x + y$ è pari se e solo se x, y sono entrambi pari o entrambi dispari. Se $x + y$ è pari e $y + z$ è pari, allora x, y, z sono tutti e tre pari o tutti e tre dispari. Di conseguenza anche $x + z$ è pari.
Le classi di equivalenza sono due: i numeri pari $\{2, 4, 6, 8, 10\}$ e i numeri dispari $\{1, 3, 5, 7, 9\}$.
N.B. La relazione di equivalenza R non è altro che la relazione di congruenza modulo 2.

(b) La relazione R non è riflessiva: infatti $x + x$ è sempre pari. Dunque non è una relazione di equivalenza.

3. *Siano dati $A = \{x, y, z, u\}$ e $B = \{1, 2, 3, 4\}$. Determinare la cardinalità dei seguenti insiemi, spiegando i ragionamenti usati:*
   $\{f : A \to B\}$, $\{f : A \to B \mid f(x) \neq f(y)\}$, $\{f : A \to B \mid \textit{iniettive}\}$, $\{f : A \to B \mid f(x) = f(y) = 1\}$.

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 $4 \cdot 4 \cdot 4 \cdot 4 = 4^4 = 256$.

(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 $4 \cdot 3 \cdot 4 \cdot 4 = 3 \cdot 4^3 = 192$.

(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 $f(x)$ e da $f(y)$, 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 $4 \cdot 3 \cdot 2 \cdot 1 = 24$.

(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 $4 \cdot 4 = 16$.

4. *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) Il numero N si fattorizza come $N = p \cdot q$ con $p = 5$ e $q = 17$. In questo caso $(p-1)(q-1) = 4 \cdot 16 = 64$. La chiave $D = 13$ soddisfa $mcd(13, 64) = 1$. Infatti

$$64 = 4 \cdot 13 + 12, \quad 13 = 1 \cdot 12 + 1.$$

Dunque appartiene a Z_{64}^*, come deve essere. La chiave E è data da $E \equiv D^{-1} \equiv 13^{-1} \bmod 64$. Per calcolarla applichiamo l'algoritmo di Euclide esteso:

$$1 \cdot 64 + 0 \cdot 13 = 64, \quad 0 \cdot 64 + 1 \cdot 13 = 13;$$

Sottraendo 4 volte la seconda relazione dalla prima, troviamo

$$1 \cdot 63 + (-4) \cdot 13 = 12;$$

infine sottraendo la terza relazione dalla seconda troviamo

$$(-1) \cdot 64 + 5 \cdot 13 = 1.$$

Dunque $\overline{13}^{-1} = \bar{5}$ in Z_{64}^* (si può verificare che $5 \cdot 13 = 65 \equiv 1 \bmod 64$). La chiave cercata è $E = 5$.

(b) Per descripatre il messaggio criptato $m = 19$, Rossi calcola $m^D \bmod N$, ossia $19^{13} \bmod 85$.

(c) per criptare il messaggio $m = 23$ da inviare al signor Rossi, si calcola $m^E \bmod N$, ossia $23^5 \bmod 85$.

5. *Determinare l'ultima cifra dei numeri 17^{13} e $(13^{13})^{17}$, spiegando bene i principi usati.*

Sol.: L'ultima cifra di un numero intero è la sua classe resto modulo 10. Quindi

$$17^{13} \equiv 7^{13} \bmod 10.$$

Osserviamo inoltre che $mcd(7, 10) = 1$, per cui $7 \in \mathbf{Z}_{10}^*$ e dal teorema di Lagrange abbiamo:

$$7^{\varphi(10)} \equiv 1 \bmod 10, \qquad \text{dove} \quad \varphi(10) = \varphi(2)\varphi(5) = 4.$$

Ne segue che

$$17^{13} \equiv 7^{13} \equiv (7^4)^3 7 \equiv 7 \bmod 10.$$

Similmente, poiché $mcd(3, 10) = 1$, vale

$$(13^{13})^{17} \equiv (3^{13})^{17} \equiv ((3^4)^3 3)^{17} \equiv 3^{17} \equiv (3^4)^4 3 \equiv 3 \bmod 10.$$

6. *In un'algebra di Boole* $(A, +, \cdot, ')$ *siano data l'espressione Booleana*

$$E: \ x'z + xyz + yz \qquad\qquad F: \ xyz + xy' + x'y'z.$$

(a) Stabilire se E *ed* F *sono equivalenti.*
(b) Scrivere F *come somma di tutti gli implicanti primi.*
(c) Scrivere F *in forma minimale.*

Sol.: Rispondiamo contemporaneamente ad (a)&(b) scrivendo E ed F come somma di tutti gli implicanti primi. Questa scrittura è unica e ci permette di confrontare E ed F. Usando la distributività e il fatto che $\alpha + 1 = 1$, per ogni $\alpha \in A$, abbiamo

$$E = x'z + xyz + yz = x'z + (x+1)yz = x'z + yz.$$

Poiché il metodo del consenso non ha "passi", $x'z + yz$ è la somma di tutti gli implicanti primi di E.

Sommando ad F il consenso tra xyz e xy', troviamo $F = xyz + xy' + x'y'z = xyz + xy' + x'y'z + xz =$
$= (y+1)xz + xy' + x'y'z = xz + xy' + x'y'z$.
Sommando a quest'ultima espressione il consenso tra xz e $x'y'z$, troviamo
$F = xz + xy' + x'y'z + y'z = xz + xy' + y'z(1 + x') =$
$= xz + xy' + y'z$.
Anche in questo caso il metodo del consenso non ha "passi" e $xz + xy' + y'z$ è la somma di tutti gli implicanti primi di F.

È evidente che E ed F non sono uguali.

(c) Per determinare una forma minimale di F, completiamo $xz + xy' + y'z$ e controlliamo se ci sono addendi superflui:

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

Non ci sono addendi superflui, quindi $xz + xy' + y'z$ è anche una forma minimale di F.