Matematica Discreta Ingegneria dei Modelli (Geatti) 1° appello Roma 30 aprile 2008, 10:00–12:00.

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 6 punti.

---

1. *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 una relazione di equivalenza o meno (giustificare).*

(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.

2. *Sia* F_n *la successione definita per ricorrenza da* $F_n = 2F_{n-1} - F_{n-2} + 2$ *con condizioni iniziali* $F_1 = 0$ *ed* $F_2 = 1$.
   (a) Determinare F_5.
   (b) Determinare F_n *risolvendo la corrispondente equazione alle differenze finite.*

(a) $F_3 = 2F_2 - F_1 + 2 = 4, \quad F_4 = 2F_3 - F_3 + 2 = 9, \quad F_5 = 2F_4 - F_3 + 2 = 16.$

(b) Soluzione generale dell'omogenea:
polinomio caratteristico $\lambda^2 - 2\lambda + 1$ con radice $\lambda = 1$ doppia, da cui

$$\alpha_n = A1^n + Bn1^n = A + nB, \qquad A, B \in \mathbf{R}.$$

Soluzione particolare:
da cercarsi del tipo $\beta_n = cn^2$. Sostituendo nell'equazione originale si trova $c = 1$, da cui:

$$\beta_n = n^2.$$

Soluzione generale dell'equazione originale:

$$F_n = A + nB + n^2, \qquad A, B \in \mathbf{R}.$$

Imponendo le condizioni iniziali $F_1 = 0$ ed $F_2 = 1$, troviamo

$$\begin{cases} A + B = -1 \\ A + 2B = -3 \end{cases} \quad \Leftrightarrow \quad A = 1, \;\; B = -2,$$

da cui la soluzione dell'equazione originale con le condizioni iniziali date risulta

$$F_n = 1 - 2n + n^2.$$

Si può controllare che effettivamente $F_5 = 16$, come previsto (cf. (a)).

3. *Determinare tutte le soluzioni dell'equazione* $\bar{x}^2 = \bar{4}$ *in* $\mathbf{Z}_{21}^*$.

Poiché $21 = 3 \cdot 7$ è prodotto di due primi maggiori di 2, l'equazione $\bar{x}^2 = \bar{4}$ ha quattro soluzioni in $\mathbf{Z}_{21}^*$. (Vedi soluzioni Esercizio 5(b)(c) Foglio 6).
Tali soluzioni sono: $\bar{x} = \bar{2}$, $\bar{x} = \overline{-2} = \overline{19}$, $\bar{x} = \bar{5}$, $\bar{x} = \overline{-5} = \overline{16}$.

4. *Il signor Rossi desidera ricevere messaggi criptati e decide di adottare il criptosistema RSA. La ditta gli fornisce un kit con chiavi pubbliche N ed E e chiave segreta D.*
   (a) La ditta gli fornisce un kit con chiavi pubbliche $N = 143$ ed $E = 23$ e chiave segreta $D = 3$. Vanno bene? (spiegare)
   (b) Preparare un kit di chiavi pubbliche N', E' e chiave segreta D' per il signor Bianchi, con $N' = 77$ ed $E' = 7$.
   (c) Spedire a Verdi, con chiavi pubbliche $N = 77$ ed $E = 7$, il messaggio $m = 13$ dopo averlo criptato.

Vedi soluzioni esonero 2

5. *Il signor Rossi e il signor Bianchi desiderano condividere un codice segreto e lo fanno adottando il sistema Merkle-Diffie-Hellman. Si accordano pubblicamente sul numero primo $p = 37$ e sulla radice primitiva $\bar{g} = \bar{2}$.*

(a) Verificare che $\bar{g} = \bar{2}$ è effettivamente una radice primitiva in $\mathbf{Z}_{37}^*$.
(b) Una spia intercetta i numeri che vengono scambiati fra Bianchi e Rossi $\overline{n} = \overline{17}$ e $\overline{m} = \overline{13}$. Cosa deve fare per ricostruire il codice segreto di Bianchi e Rossi?
(c) La spia ricostruisce il codice segreto. Qual è questo codice?

Vedi soluzioni esonero 2