ALGEBRA E LOGICA (Pareschi e Schoof) 1^{o} appello Roma 2 maggio 2002, 14:00–15:45.

COGNOME .... *NOME* ....

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare ed essenziali.* NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 5 punti.

1. Sia $n = 77$ il modulo di un sistema crittografico RSA. Sia $D = 13$ l'esponente segreto. Determinare un esponente $E \in \mathbf{Z}$ tale che $(x^D)^E \equiv x \pmod{n}$ per il messaggio $x = 4$.

Abbiamo che $n = p \cdot q$ con $p = 7$ e $q = 11$. Siccome $(p-1)(q-1) = 60$, ogni esponente $E > 0$ che soddisfa $DE = 13E \equiv 1 \pmod{60}$ va bene. Tale esponente si trova calcolando il mcd di 13 e 60. Si trova che $37 \cdot 13 \equiv 1 \pmod{60}$ e possiamo prendere $E = 37$.

2. Trovare tutte le soluzioni $x \in \mathbf{Z}$ del sistema di congruenze $\begin{cases} x \equiv 2 \pmod{5}; \\ x \equiv 3 \pmod{4}; \\ x \equiv 4 \pmod{11}. \end{cases}$

Applicando il Teorema Cinese del Resto, si trova che $x \equiv 147 \pmod{220}$.

3. Determinare quanti sono i numeri $0 \leq n < 2000$ le cui cifre hanno somma uguale a 8.

Ogni numero con questa proprietà ha tre cifre o ha la prima cifra uguale a 1. Ci sono $\binom{8+3-1}{8} = \binom{10}{2}$ numeri del primo tipo e $\binom{7+3-1}{7} = \binom{9}{2}$ del secondo. Ci sono quindi $\binom{10}{2} + \binom{9}{2} = 81$ numeri con la proprietà richiesta.

4. Sia $A = \{a, b, c, d, e\}$. Determinare la chiusura transitiva della relazione R che consiste nelle coppie (a, b), (a, e), (b, c), (c, d), (d, b).

La matrice A associata alla relazione e le sue "potenze" $A^{[2]}$ e $A^{[3]}$ sono

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad A^{[2]} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad A^{[3]} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Siccome le matrici $A^{[4]}$ e $A^{[5]}$ contengono solo ripetizioni, la chiusura transitiva di R è l'unione di R e l'insieme $\{(a, c), (b, d), (c, b), (d, c), (a, d), (b, b), (c, c), (d, d)\}$.

5. Siano x, y variabili booleane. L'operatore NAND è definito da x NAND $y = \overline{(xy)}$. Usando solo porte NAND costruire un circuito con input x e y e output $\overline{x}$ e $x + y$.

Abbiamo che $\overline{x} = x \,\mathrm{NAND}\, x$ e $xy = \overline{\overline{(xy)}} = \overline{(xy)} \,\mathrm{NAND}\, \overline{(xy)} = (x \,\mathrm{NAND}\, y) \,\mathrm{NAND}\, (x \,\mathrm{NAND}\, y)$.

6. I grafi.

Il grafo "cubo" Q_3 è bipartito. Nelle altre versioni del compito, i due grafi sono sempre isomorfi, eccetto nel caso dei due grafi "ottagonali". Essi non sono isomorfi perché un grafo contiene un vertice di grado 2 con due vertici vicini di grado 3, ma l'altro no.