ALGEBRA E LOGICA (Pareschi e Schoof) 2º appello Roma 7 maggio 2003, 14:00–16:00.

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. Usando il sistema RSA, si supponga che il modulo dell'utente sia $n = 7 \cdot 11$ e che l'esponente pubblico sia $D = 29$. Determinare l'esponente segreto E che consente di decifrare i messaggi. In altre parole, determinare un numero naturale E tale che $(a^D)^E \equiv a \pmod{n}$ per ogni a tale che $\mathrm{mcd}(a, n) = 1$.

   (a) Ogni soluzione $E \in \mathbf{N}$ della congruenza $E \cdot 29 \equiv 1 \pmod{6 \cdot 10}$ va bene. Per trovare una soluzione, si applica l'algoritmo Euclideo:

   $$\begin{aligned} 1 \cdot 60 + 0 \cdot 29 &= 60, \\ 0 \cdot 60 + 1 \cdot 29 &= 29, \\ 1 \cdot 60 - 2 \cdot 29 &= 2, \\ -14 \cdot 60 + 29 \cdot 29 &= 1. \end{aligned}$$

   L'esponente cercato è quindi $E = 29$.

2. I numeri di Fibonacci F_n sono definiti da $F_0 = 1$, $F_1 = 1$ e induttivamente da $F_n = F_{n-1} + F_{n-2}$ per $n \geq 2$.
   (a) Calcolare F_5.
   (b) Dimostrare per induzione che $\mathrm{mcd}(F_{n-1}, F_n) = 1$ per ogni $n \geq 1$.

   (a) $F_2 = F_0 + F_1 = 2$, $F_3 = F_1 + F + 2 = 3$, $F_4 = F_2 + F_3 = 5$, $F_5 = F_3 + F_4 = 8$.
   (b) $n = 1$: $\mathrm{mcd}(F_0, F_1) = \mathrm{mcd}(1, 1) = 1$.
   Passo induttivo: supponiamo che $\mathrm{mcd}(F_{n-1}, F_n) = 1$. Si deve dimostrare che $\mathrm{mcd}(F_n, F_{n+1}) = 1$. Sia m un numero naturale che divide sia F_n che $F_{n+1} = F_n + F_{n-1}$. Allora m divide anche la differenza $F_{n+1} - F_n = F_{n-1}$. Quindi m divide sia F_n che F_{n-1} e dunque, per l'ipotesi induttiva, $m = 1$. L'asserzione è dimostrata.

3. Sia $n = 55 = 5 \cdot 11$. Determinare le classi di congruenza $x \in \mathbf{Z}_n$ che soddisfano $x^2 \equiv 1 \pmod{n}$.

   Per un primo $p > 2$ abbiamo che $x^2 \equiv 1 \pmod{p}$ se e soltanto se $x \equiv \pm 1 \pmod{p}$. Questo segue dal fatto che se p divide $x^2 - 1 = (x - 1)(x + 1)$, allora p divide $x - 1$ oppure p divide $x + 1$. Abbiamo che $55 = 5 \cdot 11$ e quindi $x \in \mathbf{Z}$ soddisfa $x^2 \equiv 1 \pmod{55}$ se e soltanto se $x^2 \equiv 1 \pmod{5}$ e $x^2 \equiv 1 \pmod{11}$. Siccome 5 e 11 sono primi, questo è equivalente a $x \equiv \pm 1 \pmod{5}$ e $x \equiv \pm 1 \pmod{11}$. I quattro sistemi di congruenze ri risolvono tramite il Teorema Cinese del Resto. Per esempio,

   $$\begin{cases} x \equiv 1 \pmod{11}, \\ x \equiv -1 \pmod{5}. \end{cases}$$

   Ha come soluzione $x \equiv 34 \pmod{55}$. In questo modo si trovano le soluzioni $x \equiv \pm 1 \pmod{55}$ e $x \equiv \pm 34 \pmod{55}$.

4. Siano x, y, z variabili Booleane.
   (a) Scrivere un'espressione Booleana E in x, y, z che corrisponde alla seguente tabella di verità.
   (b) Trovare una forma minimale per l'espressione della parte (a).

x	y	z	E
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Un'espressione Booleana E corrispondente alla tabella è data dalla forma normale disgiuntiva: $\overline{x}\,\overline{y}\,\overline{z}+x\overline{y}\,\overline{z}+x\overline{y}z$. Per trovare una forma minimale, applichiamo il metodo del consenso: $x\overline{y}\,\overline{z}+x\overline{y}z = x\overline{y}\,\overline{z}+x\overline{y}z+x^2\overline{y}^2 = x\overline{y}\,\overline{z}+x\overline{y}z+x\overline{y} = x\overline{y}$. E quindi $E = \overline{x}\,\overline{y}\,\overline{z}+x\overline{y}$, Riapplicando il metodo del consenso troviamo che $E = \overline{x}\,\overline{y}\,\overline{z}+x\overline{y}+\overline{y}^2\overline{z} = \overline{x}\,\overline{y}\,\overline{z}+x\overline{y}+\overline{y}\overline{z} = x\overline{y}+\overline{y}\,\overline{z}$.

5. Sia $A = \mathbf{R} - \{0\}$. Considerare le seguenti relazioni su A:

$$aR_1b, \qquad \text{se e soltanto se } a \cdot b < 0;$$
$$aR_2b, \qquad \text{se e soltanto se } a \cdot b = 0;$$
$$aR_3b, \qquad \text{se e soltanto se } a \cdot b > 0;$$

Stabilire se R_1, R_2 e R_3 sono relazioni di equivalenza o meno. In caso affermativo, stabilire quante sono le classi di equivalenza e descriverle.

La relazione R_1 non è riflessiva: se $a \in \mathbf{R} - \{0\}$ si ha che $a \cdot a > 0$ e quindi a non è in relazione con a. Dunque R_1 non è una relazione di equivalenza. (Alternativamente si può verificare che R_1 non è transitiva).
La relazione R_2 non è riflessiva: se $a \in \mathbf{R} - \{0\}$ si ha che $a \cdot a > 0$ e quindi a non è in relazione con a. Dunque R_2 non è una relazione di equivalenza.
La relazione R_3 è riflessiva: per ogni $a \in \mathbf{R} - \{0\}$ si ha che $a \cdot a > 0$ e dunque aR_3a. La relazione R_3 è simmetrica: $a \cdot b > 0 \Leftrightarrow b \cdot a > 0$. Dunque $aR_3b \Rightarrow bR_3a$.
La relazione R_3 è transitiva. Per verificare ciò si può osservare che $a \cdot b > 0$ è equivalente al fatto che a e b hanno lo stesso segno. Dunque se a ha lo stesso segno di b e b ha lo stesso segno di c, a ha lo stesso segno di c. Quindi aR_3b e $bR_3c \Rightarrow aR_3c$.
Da quanto sopra segue che, dato $a \in \mathbf{R} - \{0\}$, la sua classe di equivalenza secondo R_3 consiste di tutti i $b \in \mathbf{R} - \{0\}$ che hanno lo stesso segno di a. Ne segue che le classi di equivalenza secondo R_3 sono due: i numeri reali positivi e i numeri reali negativi.

6. Definiamo su $\mathbf{N}$ la relazione $a \leq b$ se e soltanto se esiste $r \in \mathbf{N}$ tale che $a^r = b$.
   (a) Dimostrare che si tratta di una relazione d'ordine parziale.
   (b) Determinare, se esistono, $\inf(36, 8)$ e $\sup(9, 27)$.

(a) Riflessività: per ogni $a \in \mathbf{N}$ $a^1 = a$. Dunque $a \leq a$. Antisimmetria: se $\exists r \in \mathbf{N}$ tale che $a^r = b$ e $\exists s \in \mathbf{N}$ tale che $b^s = a$ allora è evidente che $r = s = 1$ e $a = b$. Dunque $a \leq b$ e $b \leq a \Rightarrow a = b$. Transitività: se $\exists r \in \mathbf{N}$ tale che $a^r = b$ e $\exists s \in \mathbf{N}$ tale che $b^s = c$ allora $a^{rs} = (a^r)^s = b^s = c$. Dunque $a \leq b$ e $b \leq c \Rightarrow a \leq c$.
(b) L'insieme dei minoranti dell'insieme $\{36\}$ è l'insieme $\{6\}$. L'insieme dei minoranti dell'insieme $\{8\}$ è l'insieme $\{2\}$. Quindi 36 e 8 non hanno minoranti comuni. In altre parole l'insieme dei minoranti di $\{36, 8\}$ è vuoto. Dunque $inf(36, 8)$ non esiste.
L'insieme dei maggioranti di 9 è l'insieme $\{9^r : r \in \mathbf{N}\} = \{3^m : m \text{ pari}\}$. L'insieme dei maggioranti di 27 è $\{27^r : r \in \mathbf{N}\} = \{3^k : k \text{ è un multiplo di } 3\}$. Dunque l'insieme dei maggioranti di $\{9, 27\}$ è $\{3^h : h \text{ è un multiplo di } 6\}$, il cui minimo è $3^6 = 729$. Dunque $sup(9, 27) = 729$.