ALGEBRA E LOGICA (Pareschi e Schoof) 1° appello Roma 30 Aprile 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. Dimostrare per induzione che $\sum_{k=1}^{n} \frac{1}{k^2} \leq 2 - \frac{1}{n}$ per ogni $n \geq 1$.

Per $n = 1$ l'affermazione è vera. Supponendo l'affermazione vera per $n \in \mathbf{N}$ facciamo adesso vedere che vale anche per $n+1$. Abbiamo che $\sum_{k=1}^{n+1} \frac{1}{k^2} = \sum_{k=1}^{n} \frac{1}{k^2} + \frac{1}{(n+1)^2}$. Dobbiamo dimostrare che questo è $\leq 2 - \frac{1}{n+1}$. Per l'ipotesi d'induzione abbiamo che $\sum_{k=1}^{n} \frac{1}{k^2} \leq 1 - \frac{1}{n}$. Basta quindi dimostrare che $2 - \frac{1}{n} + \frac{1}{(n+1)^2} \leq 2 - \frac{1}{n+1}$. Questo segue dal fatto che $\frac{1}{(n+1)^2} \leq \frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$.

2. Sia $X = \{n \in \mathbf{Z} : 1 \leq n \leq 34\}$ e sia R la relazione su X definita nel modo seguente: nRm se e solo se n e m hanno lo stesso numero di cifre in base 2 (cioè se le rappresentazioni in base 2 di n e m hanno la stessa lunghezza).
   (a) Stabilire se R è una relazione di equivalenza;
   (b) In caso affermativo, determinare quante sono le classi di equivalenza e descriverle.

Ogni numero ha lo stesso numero di cifre che se stesso. Se n e m hanno lo stesso numero di cifre, vale anche il viceversa. Se m ha lo stesso numero di cifre di n e n ha lo stesso numero di cifre di p, allora m ha lo stesso numero di cifre di p. In conclusione: R è una relazione di equivalenza. Le classi di equivalenza sono i sottoinsiemi di X che consistono degli n che hanno lo stesso numero di cifre. Siccome 34 è uguale a 100001 in base 2, il numero di cifre dei numeri $n \in X$ varia fra 1 e 6. Ci sono quindi 6 classi di equivalenza.

3. Siano $X = \{n \in \mathbf{Z} : n < -10\}$ e $Y = \{n \in \mathbf{Z} : n \geq 5\}$. Esibire una funzione biettiva $f : X \cup Y \to \mathbf{Z}$.

Una biezione $f : X \cup Y \longrightarrow \mathbf{Z}$ è data da

$$f(n) = n, \qquad \text{se } n \in X,$$
$$f(n) = n - 15, \qquad \text{se } n \in Y.$$

4. Si consideri il sistema crittografico RSA corrispondente al modulo $n = 143 = 11 \cdot 13$ e all'esponente $D = 53$.
   (a) Cifrare il messaggio "24", cioè calcolare il resto della divisione per 143 del numero 24^{53} (suggerimento: calcolare il resto delle divisioni per 11 e per 13 del numero 24^{53});
   (b) Determinare un esponente E che consente di decifrare il messaggio precedente. In altre parole: determinare un numero naturale E tale che $(24^{53})^E \equiv 24 \pmod{143}$.

   (a) Siccome $53 \equiv 3 \pmod{10}$, abbiamo per il Teorema di Fermat che $x = 24^{53} \equiv 2^3 \equiv 8 \pmod{11}$. Similmente, $53 \equiv 5 \pmod{12}$ e quindi $x = 24^{53} \equiv (-2)^5 \equiv -32 \equiv 7 \pmod{13}$. Con il Teorema Cinese del resto si trova che $x \equiv 85 \pmod{143}$. (b) Ogni soluzione $E \in \mathbf{N}$ della congruenza $E \cdot 53 \equiv 1 \pmod{10 \cdot 12}$ va bene. Per trovare una soluzione, si applica l'algoritmo Euclideo:

$$\begin{aligned}
1 \cdot 120 + \ 0 \cdot 53 &= 120,\\
0 \cdot 120 + \ 1 \cdot 53 &= 53,\\
1 \cdot 120 - \ 2 \cdot 53 &= 14,\\
-3 \cdot 120 + \ 7 \cdot 53 &= 11,\\
4 \cdot 120 - \ 9 \cdot 53 &= 3,\\
-15 \cdot 120 + 34 \cdot 53 &= 2,\\
19 \cdot 120 - 43 \cdot 53 &= 1.
\end{aligned}$$

   L'esponente cercato è quindi $E = -43 + 120 = 77$.

5. Sia $f : \mathbf{N} \to \mathbf{Z}$ una funzione fissata.
   (a) Esprimere la proposizione "*f è iniettiva*" usando quantificatori e connettivi logici.
   (b) Esprimere la proposizione "*f non è iniettiva*" usando quantificatori e connettivi logici, in modo tale che non ci siano negazioni davanti a quantificatori.

   (a) $\forall x \in \mathbf{N} \forall y \in \mathbf{N} \ x \neq y \to f(x) \neq f(y)$
   oppure: $\forall x \in \mathbf{N} \forall y \in \mathbf{N} \ f(x) = f(y) \to x = y$.
   (b) $\exists x \in \mathbf{N} \exists y \in \mathbf{N} (x \neq y) \wedge (f(x) = f(y))$

6. In un'algebra di Boole si consideri l'operazione $x \oplus y := xy' + x'y$.
   (a) Esprimere l'espressione booleana $(xy) \oplus (z \oplus x')$ come somma di prodotti.

   (a) $(xy) \oplus (z \oplus x') = (xy)(z \oplus x')' + (xy)'(z \oplus x')$
   $\overset{DN}{=} (xy)(zx + z'x')' + (xy)'(zx + z'x')$
   $\overset{DM}{=} (xy)(zx)'(z'x')' + (x' + y')(zx + z'x')$
   $\overset{DM+DN}{=} (xy)(z' + x')(z + x) + (x' + y')(zx + z'x')$
   $\overset{D}{=} xyz'z + xyz'x + xyx'z + xyx'x + x'zx + x'z'x' + y'zx + y'z'x'$
   $\overset{C+Co+I}{=} xy0 + xyz' + 0yz + 0xy + 0z + x'z' + xy'z + x'y'z'$
   $\overset{L}{=} xyz' + x'z' + xy'z + x'y'z' \overset{A}{=} xyz' + x'z' + xy'z.$

   (dove: DN=doppia negazione, DM=De Morgan, D=distributività, C=commutatività, Co=complemento, I=idempotenza, L= limitatezza, A=assorbimento).

   (Alternativamente, si può pervenire al risultato trovando esplicitamente la "tabella di verità" dell'espressione, pervenendo direttamente alla espressione in somma di prodotti completata: $xyz' + x'yz' + x'y'z' + xy'z$.)