ALGEBRA E LOGICA (Pareschi e Schoof) 1^o esonero Roma 31 marzo 2003, 16:00–18:00.

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. Sia X l'insieme dei sottoinsiemi $A \subset \{1,2,3,4,5\}$ tali che $|A|$ è dispari (dove $|A|$ denota il numero di elementi di A). Sia $R \subset X \times X$ la relazione data da $\big\{(A,B) \in X \times X \mid A \subset B\big\}$.
   (a) Dimostrare che R è una relazione d'ordine parziale;
   (b) Esibire, se possibile, A e B tali che $|A| = |B| = 3$ e tali che $inf\{A,B\}$ non esiste;
   (c) Esibire, se possibile, A e B tali che $|A| = |B| = 3$ e tali che $inf\{A,B\}$ esiste.

(a) Per ogni $A \in X$ abbiamo che $A \subset A$ e quindi $(A,A) \in R$. Se (A,B) e (B,A) appartengono ad R, allora $A \subset B$ e $B \subset A$ e quindi $A = B$. Infine, se $(A,B) \in R$ e $(B,C) \in R$, allora $A \subset B \subset C$ e quindi $A \subset C$, cioè $(A,C) \in R$. Concludiamo che R è un ordinamento parziale.
(b) Per esempio $A = \{1,2,3\}$ e $B = \{2,3,4\}$. Allora i minoranti in X di A e B sono $\{2\}$, $\{3\}$. L'insieme dei minoranti non possiede quindi un minimo assoluto e $inf\{A,B\}$ non esiste.
(c) Il minorante di $A = \{1\}$ e $B = \{1\}$ è $\{1\}$ stesso. Alternativamente, il minorante di $A = \{1,2,3\}$ e $B = \{3,4,5\}$ è l'insieme $\{3\}$.

2. Sia X l'insieme dei numeri naturali pari. Esibire una funzione biettiva $f : \mathbf{Z} \to X$.

La funzione $f : \mathbf{Z} \longrightarrow X$ definita da $f(k) = 4k$ per $k > 0$ e $f(k) = 2-4k$ per $k \leq 0$ è una biezione. Per dimostrare l'iniettività supponiamo che $f(k) = f(k')$. Ci sono due possibilità. Se $f(k) = f(k') \equiv 0 \pmod 4$, allora $4k = f(k) = f(k') = 4k'$ e quindi $k = k'$. Oppure $f(k) = f(k') \not\equiv 0 \pmod 4$ e quindi $4k+2 = f(k) = (k') = 4k'+2$ e quindi $k = k'$. Per dimostare la suriettività, sia $m \in X$ un numero pari. Se m è divisibile per 4 allora $f(m/4) = m$. Se no, allora $m \equiv 2 \pmod 4$ e $f(\frac{2-m}{4}) = m$.

3. Sia $T = \{(a,b) \in \mathbf{R}^2 : a \neq 0 \text{ e } b \neq 0\}$. Sia $R \subset T \times T$ la relazione
$$R = \{((a,b),(a',b')) \in T \times T : aa' > 0 \text{ e } bb' > 0\ \}.$$
   (a) Dimostrare che R è una relazione di equivalenza.
   (b) Descrivere le classi di equivalenza. Quante sono?

(a) - per ogni $(a,b) \in T$ si ha che $((a,b),(a,b)) \in R$. Infatti $aa > 0$ e $bb > 0$. quindi la relazione è riflessiva.
- se $((a,b),(a',b')) \in R$ allora $((a',b'),(a,b)) \in R$. Infatti se $aa' > 0$ e $bb' > 0$ allora anche $a'a > 0$ e $b'b > 0$. Quindi la relazione è simmetrica.
- se $(a,b),(a',b')) \in R$ e $(a',b'),(a'',b'') \in R$ allora $((a,b),(a'',b'')) \in R$. Infatti il prodotto di due numeri reali (diversi da zero) è positivo se e solo se i due numeri hanno lo stesso segno. Quindi l'implicazione precedente significa se a e a' (risp. b e b') hanno lo stesso segno e a' e a'' (risp. b' e b'') hanno lo stesso segno allora anche a e a'' (risp. b e b'') hanno lo stesso segno, il che è chiaramente vero. Alternativamente, si può notare che che moltiplicando membro a membro le disuguglianze $aa' > 0$ e $a'a'' > 0$ si ottiene $aa'^2a'' > 0$, che è equivalente a $aa'' > 0$ perché $a'^2 > 0$. Lo stesso per la seconda coordinata.
(b) Da quanto sopra risulta che due coppie sono in relazione se e solo se le loro prime coordinate hanno lo stesso segno e le loro seconde coordinate hanno lo stesso segno. Ne consegue che le classi di equivalenza sono quattro: $\{(a,b) \in T : a > 0, b > 0\}$, $\{(a,b) \in T : a > 0, b < 0\}$, $\{(a,b) \in T : a < 0, b > 0\}$, $\{(a,b) \in T : a < 0, b < 0\}$, cioè i quattro quadranti.

4. Dimostrare per induzione che $\sum_{k=0}^{n-1} \frac{1}{(2k+1)(2k+3)} = \frac{n}{2n+1}$ per ogni $n \geq 1$.

Per $n = 1$, la somma ha solo il termine con $k = 0$ ed è uguale a $1/3 = n/(2n+1)$. Supponiamo adesso che la fomula valga per n e cerchiamo di dimostrarla per $n + 1$. Per induzione abbiamo che

$$\sum_{k=0}^{n} \frac{1}{(2k+1)(2k+3)} = \sum_{k=0}^{n-1} \frac{1}{(2k+1)(2k+3)} + \frac{1}{(2n+1)(2n+3)},$$
$$= \frac{n}{2n+1} + \frac{1}{(2n+1)(2n+3)} = \frac{n(2n+3)+1}{(2n+1)(2n+3)} = \frac{n+1}{2n+3}$$

come richiesto.

5. Determinare i numeri naturali n di tre cifre decimali che soddisfano $n \equiv 6 \pmod 7$, $n \equiv 1 \pmod{11}$, $n \equiv 3 \pmod 5$.

Primo metodo: la prima equazione ci dice che $n = 6+7h$ per $h \in \mathbf{Z}$. Sostituendo questo nella seconda equazione, troviamo che $6 + 7h \equiv 1 \pmod{11}$ e quindi che $7h \equiv -5 \pmod{11}$. Si vede facilmente che $h \equiv 4 \pmod{11}$. In altre parole, $h = 4+11k$ per $k \in \mathbf{Z}$. Sostituendo questa espressione troviamo che $n = 6+7h = 6 + 7(4 + 11k) = 34 + 77k$. Sostituendo questo nella terza congruenza, troviamo che $34 + 77k \equiv 3 \pmod 5$ e quindi che $2k \equiv 4 \pmod 5$, cioè $k \equiv 2 \pmod 5$. In altre parole $k = 2 + 5m$ per $m \in \mathbf{Z}$. Sostituendo troviamo che $n = 34 + 77k = 34 + 77(2 + 5m) = 188 + 385m$ per $m \in \mathbf{Z}$. Per $m = 0, 1, 2$ troviamo numeri naturali di tre cifre: $n = 188$, 573, 958.

Secondo metodo: Usando l'algoritmo Euclideo, si trova l'equazione $(-3) \cdot 7 + 2 \cdot 11 = 1$. Le soluzioni delle prime due congruenze sono quindi $n \equiv -3 \cdot 7 \cdot 1 + 2 \cdot 11 \cdot 6 = 111 \equiv 34 \pmod{77}$. Usando l'algoritmo Euclideo una seconda volta, si trova che $(-2) \cdot 77 + 31 \cdot 5 = 1$ e quindi le soluzioni comuni delle congruenze $n \equiv 34 \pmod{77}$ e $n \equiv 3 \pmod 5$ sono $n = -2 \cdot 77 \cdot 3 + 31 \cdot 5 \cdot 34 = 4808 \equiv 188 \pmod{385}$. Le soluzioni di tre cifre si trovano come sopra.

6. Determinare il resto della divisione per 11 del numero $8^{11^{11}}$.

Per il piccolo Teorema di Fermat (oppure per il Teorema di Lagrange), abbiamo che $8^a \equiv 8^b \pmod{11}$ quando $a \equiv b \pmod{10}$. Basta quindi calcolare l'esponente 11^{11} modulo 10. Siccome $11 \equiv 1 \pmod{10}$, abbiamo che anche $11^{11} \equiv 1 \pmod{10}$. Quindi $8^{11^{11}} \equiv 8^1 = 8 \pmod{10}$.