ALGEBRA E LOGICA (Pareschi e Schoof) 4º Appello Roma, 18 settembre 2002, 13:45–16:00.

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

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare ed essenziali.* NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 6 punti.

1. Siano p, q ed r tre proposizioni. Scrivere in forma normale disgiunta

$$(q \to (p \to q)) \to r.$$

p	q	r	$q \to p$	$(q \to p) \to q$	$((q \to p) \to q) \to r$
0	0	0	1	0	1
0	0	1	1	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	1
1	1	0	1	0	1
1	0	1	1	1	0
1	1	1	1	1	1

Calcolando la tabella di verità, si trova che una forma normale disgiunta della proposizione data è

$$(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r).$$

2. Sia $n = 77$ il modulo di un sistema crittografico RSA. Sia $D = 17$ l'esponente segreto. Determinare un esponente positivo $E \in \mathbf{Z}$ tale che $(x^D)^E \equiv x \pmod{n}$ per il messaggio $x = 5$.

Abbiamo che $n = pq$ con $p = 11$ e $q = 7$. Per il Teorema di Fermat, ogni $E \in \mathbf{Z}$ che soddisfa $DE \equiv 1 \pmod{(p-1)(q-1)}$ ha la proprietà richiesta. Si risolve la congruenza $17E \equiv 1 \pmod{60}$ calcolando il $\mathrm{mcd}(17, 60)$. Il risultato è che $E \equiv -7 \pmod{60}$. In altre parole, $E = -7 + 60k$ con $k \in \mathbf{Z}$. Per $k = 1$ troviamo un numero positivo: $E = 53$.

3. Determinare tutti numeri naturali n di tre cifre, con ultima cifra uguale a 7, tali che il resto della divisone di n per 3 sia uguale a 1 e il resto della divisone di n per 11 sia uguale a 2.

La prima condizione dice esattamente che $n \equiv 7 \pmod{10}$. Così troviamo un sistema di tre congruenze:

$$\begin{cases} n \equiv 7 \pmod{10} \\ n \equiv 1 \pmod{3} \\ n \equiv 2 \pmod{11} \end{cases}.$$

Usando il Teorema Cinese del resto, si trova che la seconda e la terza conguenza equivalgono alla singola congruenza $n \equiv 13 \pmod{33}$. Una seconda applicazione del Teorema Cinese del resto a questa conguenza e la conguenza $n \equiv 7 \pmod{10}$ ci da che n è congruo a 277 modulo 330. In altre parole, $n = 277 + 330k$ con $k \in \mathbf{Z}$. Solo per $k = 0$, 1 e 2 il numero n ha tre cifre: $n = 277$, 607 e 937.

4. Sia P l'insieme delle parti di $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Per $A, B \in P$, definiamo $A \sim B$ quando A e B hanno lo stesso numero di elementi.
   (i) Dimostrare che si tratta di una relazione di equivalenza.
   (ii) Quante classi di equivalenza ci sono?

(i) La relazione è riflessiva, perché ogni insieme A contiene lo stesso numero di elementi di se stesso. La relazione è simmetrica, perché se A contiene lo stesso numero di elementi di B, allora B contiene lo stesso numero di elementi di A. La relazione è transitiva, perché se A contiene lo stesso numero di elementi di B e B contiene lo stesso numero di elementi di C, allora A contiene lo stesso numero di elementi di C.

(ii) Le classi di equivalenza sono i sottoinsiemi P_k di P che contengono i sottoinsiemi A di cardinalità k. Ce n'è una per ogni k fra 0 e 10. Ci sono quindi 11 classi di equivalenza.

5. Sia $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Per $x, y \in S$, definiamo $x \leq y$ quando x divide y e allo stesso tempo $x + y$ è pari.
   (i) Dimostrare che si tratta di un ordinamento parziale.
   (ii) Determinare gli elementi massimali.

(i) Osserviamo prima che $x + y$ è pari se e soltanto se x e y hanno la stessa parità. La relazione è riflessiva, perché ogni numero x divide se stesso e ha la stessa parità di se stesso. La relazione è antisimmetrica, perché se $x \leq y$ e $y \leq x$, allora in particolare x divide y e y divide xe quindi $x = y$. La relazione è transitiva, perché se $x \leq y$ e $y \leq z$, allora x divide y e y divide z e quindi x divide z. Inoltre, x e y hanno la stessa parità, y e z hanno la stessa parità e quindi x ha la stessa parità di z. Questo implica che $x \leq z$.

(ii) Il diagramma di Hasse ha due componenti: gli elementi pari e quelli dispari. Gli elementi massimali sono 5, 6, 7, 8, 9 e 10 perché non dividono nessun altro elemento di S della stessa parità.