ALGEBRA E LOGICA (Pareschi e Schoof) 4º appello Roma 24 settembre 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 6 punti.

1. Trovare una formula generale per la somma $1 + 2 + 4 + 8 + 16 + \ldots + 2^n$. Dimostrare per induzione che la formula trovata è quella giusta.

Si tratta di una serie geometrica. Per $n = 1, 2, 3, 4, \ldots$ si trova che la somma è uguale rispettivamente a 3, 7, 15, 31, ... e si riconoscono le potenze di 2 meno 1. La formula cercata è quindi $1 + 2 + 4 + 8 + 16 + \ldots + 2^n = s_n = 2^{n+1} - 1$.

Dimostriamo la validità della formula per induzione: per $n = 1$ abbiamo che $1 + 2 = s_1 = 2^2 + 1$. Questo è corretto. Supponendo che la formula valga per n, abbiamo che $s_{n+1} = s_n + 2^{n+1} = (2^{n+1} - 1) + 2^{n+1} = 2^{n+2} - 1$. Vediamo che la formula vale anche per $n + 1$, come richiesto.

2. Determinare l'ultima cifra decimale di 5^{6^7} e di 7^{6^5}. (Ricordiamo che a^{b^c} è uguale a $a^{(b^c)}$).

Nel primo caso osserviamo che $5 \cdot 5 \equiv 5 \pmod{10}$. In parole povere: un prodotto di due numeri con ultima cifra decimale uguale a 5 ha lui stesso l'ultima cifra uguale a 5. Siccome 5^{6^7} è prodotto di 6^7 fattori uguali a 5, anche 5^{6^7} ha l'ultima cifra uguale a 5.

Nel secondo caso, osserviamo che $10 = 2 \cdot 5$ e usiamo il teorema cinese del resto. Per il teorema di Fermat (o facendo il calcolo) abbiamo che $7^4 \equiv 1 \pmod 5$. Siccome l'esponente 6^7 è divisibile per 4, abbiamo che $7^{6^5} \equiv 1 \pmod 5$. Siccome 7 è dispari, ogni potenza di 7 è dispari. In particolare, abbiamo che $7^{6^5} \equiv 1 \pmod 2$. L'ultima cifra cercata è quindi congrua a 1 (mod 5) ed anche congrua a 1 (mod 2). Usando il teorema cinese (o direttamente) si trova che la cifra deve essere uguale a 1.

3. Sia $A = \{0, 1, 2\}$ e sia $P(A)$ l'insieme delle parti di A. Spiegare se esiste o meno una biezione da $P(A)$ all'insieme $\{(a, b) \in A \times A : a + b > 0\}$. Se esiste, esibirne una.

Siccome A ha 3 elementi, l'insieme $P(A)$ ne ha $2^3 = 8$. Il prodotto $A \times A$ ha $3 \cdot 3 = 9$ elementi. Il suo sottoinsieme $\{(a, b) \in A \times A : a + b > 0\}$ ha quindi 8 elementi perché è uguale ad $A \times A$, tolta la coppia $(0, 0)$.

Poiché i due insiemi hanno lo stesso numero di elementi, esiste una biezione fra essi. Infatti ne esistono tante (32320 per essere precisi). Eccone un esempio: la biezione g definita da

$$\begin{aligned} g(\emptyset) &= (0,1), \\ g(\{0\}) &= (0,2), \\ g(\{1\}) &= (1,0), \\ g(\{0,1\}) &= (1,1), \\ g(\{2\}) &= (1,2), \\ g(\{0,2\}) &= (2,0), \\ g(\{1,2\}) &= (2,1), \\ g(A) &= (2,2). \end{aligned}$$

4. Usando il sistema RSA, supponiamo 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 $\operatorname{mcd}(a, n) = 1$.

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 $E = 29$.

5. 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 $E = \overline{x}\,\overline{y}\,\overline{z} + x\overline{y} + \overline{y}^2\overline{z} = \overline{x}\,\overline{y}\,\overline{z} + x\overline{y} + \overline{y}\overline{z} = x\overline{y} + \overline{y}\,\overline{z}$.

6. Sia $\mathbf{Z}_7^*$ il gruppo moltiplicativo dei resti non nulli modulo 7.
   (a) Dimostrare che $\overline{2} \in \mathbf{Z}_7^*$ è un quadrato. In altre parole, dimostrare che esiste $\overline{a} \in \mathbf{Z}_7^*$ tale che $\overline{a}^2 = \overline{2}$ in $\mathbf{Z}_7^*$.
   (b) Dimostrare che $\overline{3} \in \mathbf{Z}_7^*$ non è un quadrato.
   (c) Per $\overline{a}, \overline{b} \in \mathbf{Z}_7^*$ definiamo la relazione $\overline{a} \sim \overline{b}$ quando $\overline{a} \cdot \overline{b}$ è un quadrato. Dimostrare che si tratta di una relazione di equivalenza.
   (d) Quante classi di equivalenza ci sono?

Abbiamo che $3^2 \equiv 2 \pmod{7}$ e quindi la parte (a) è chiara.

Per dimostrare (b) calcoliamo tutti i quadrati modulo 7. Osservando che $4 \equiv -3 \pmod{7}$, $5 \equiv -2 \pmod{7}$ e $6 \equiv -1 \pmod{7}$, troviamo che i quadrati in $\mathbf{Z}_7^*$ sono $(\pm 1)^2 \equiv 1 \pmod{7}$, $(\pm 2)^2 \equiv 4 \pmod{7}$ e $(\pm 3)^2 \equiv 2 \pmod{7}$. Il sottoinsieme dei quadrati è quindi uguale a $\{\overline{1}, \overline{2}, \overline{4}\} \subset \mathbf{Z}_7^*$. Siccome $\overline{3}$ non appartiene a questo sottoinsieme, $\overline{3}$ non è un quadrato.

Siccome $\overline{a} \cdot \overline{a} = \overline{a}^2$ è sempre un quadrato, la relazione è riflessiva. Se $\overline{a} \cdot \overline{b}$ è un quadrato, anche $\overline{b} \cdot \overline{a}$ lo è, perché $\overline{b} \cdot \overline{a} = \overline{a} \cdot \overline{b}$. La relazione è quindi simmetrica. Finalmente, se $\overline{a} \cdot \overline{b}$ e $\overline{b} \cdot \overline{c}$ sono quadrati, anche il prodotto $\overline{a} \cdot \overline{b}^2 \cdot \overline{c}$ lo è. Moltiplicando per il quadrato dell'inverso di $\overline{b}$ segue che anche $\overline{a} \cdot \overline{c}$ è un quadrato. Questo implica la transitività della relazione. Si tratta quindi di una relazione di equivalenza.

Ci sono due classi di equivalenza: i quadrati $\{\overline{1}, \overline{2}, \overline{4}\}$ e i non quadrati $\{\overline{3}, \overline{5}, \overline{6}\}$.