ALGEBRA E LOGICA (Geatti) 1^o appello Roma, 8 febbraio 2010, ore 10:00–12:00.

Cognome .... **Nome** ....

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare e sintetiche.*
NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 5 punti.

1. *Siano A e B insiemi e sia $f\colon A \to B$ una funzione.*
   (a) Richiamare la definizione di funzione iniettiva.
   (b) Determinare se la funzione $f\colon\ \mathbb{Z} \to\ \mathbb{Z}$, data da $f(n) = 3+5n^2$ è iniettiva. È suriettiva? (spiegare).
   (c) Determinare l'immagine tramite f dell'insieme $\{x \in\ \mathbb{Z},\ -5 \le x \le 2\}$.

(a) Leggi le dispense!!
(b) La funzione data non è iniettiva perché esistono interi distinti $n \neq m \in\ \mathbb{Z}$ con $f(n) = f(m)$, ossia con la stessa immagine tramite f. Ad esempio, per $n = 1$ ed $m = -1$ vale $f(n) = 3+5\cdot 1^2 = f(m) = 3+5\cdot(-1)^2 = 8$.
(c) L'immagine tramite f dell'insieme $\{x \in\ \mathbb{Z},\ -5 \le x \le 2\}$ è uguale all'immagine dell'insieme $\{x \in\ \mathbb{Z},\ 0 \le x \le 2\}$ (perché interi di segno opposto hanno la stessa immagine):

$$f(\{x \in\ \mathbb{Z},\ -5 \le x \le 2\}) = f(\{x \in\ \mathbb{Z},\ -5 \le x \le 0\}) =$$
$$= \{f(0), f(1) = f(-1), f(2) = f(-2), f(-3), f(-4), f(-5)\} = \{3, 8, 23, 48, 83, 128\}.$$

2. *Sia $A = \{1, 3, 5, 7, 9, 11, 23, 33, 35, 42, 45\}$ e su A si consideri la relazione data da "$a\ R\ b$ se a e b hanno la somma delle cifre uguale".*
   (a) Verificare che R è una relazione di equivalenza.
   (b) Determinare le classi di equivalenza (elencandone gli elementi).

Scriviamo un generico elemento di A come $X = x_1x_2$, con la convenzione che $x_1 = 0$ se $X \le 9$.
(a) R è riflessiva: XRX, in quanto $x_1 + x_2 = x_1 + x_2$;
R è simmetrica: $\forall X, Y \quad XRY \Rightarrow YRX$ in quanto $x_1 + x_2 = y_1 + y_2 \Rightarrow y_1 + y_2 = x_1 + x_2$.
R è transitiva: $\forall X, Y, Z \quad \begin{cases} XRY \\ YRZ \end{cases} \Rightarrow XRZ$. Infatti se $x_1 + x_2 = y_1 + y_2$ e $y_1 + y_2 = z_1 + z_2$, allora anche $x_1 + x_2 = z_1 + z_2$.
(b) Le classi di equivalenza indotte dalla relazione R su A contengono elementi con somma delle cifre uguali:

$$[1] = \{1\},\ [3] = \{3\},\ [5] = \{5, 23\},\ [7] = \{7\},\ [9] = \{9, 45\},\ [11] = \{11\},\ [33] = \{33, 42\},\ [35] = \{35\}.$$

Sono una famiglia di sottoinsiemi di A non vuoti, disgiunti, la cui unione esaurisce tutto A; sono cioè una partizione di A.

3. (a) *Determinare tutte le soluzioni $x \in\ \mathbb{Z}$ della congruenza* $3x \equiv 4 \bmod 11$.
   (b) Determinare le soluzioni comprese nell'intervallo $[-5, 20]$.

(a) Poiché $\mathrm{mcd}(3, 11) = 1$ e 1 divide 4, la congruenza ha soluzioni intere. Tutte e sole le soluzioni sono della forma $x = x_0 + k11$, dove $x_0 \in\ \mathbb{Z}$ è una qualunque soluzione particolare della congruenza e $k \in\ \mathbb{Z}$. Per determinare una soluzione particolare x_0 determiniamo a e b interi tali che

$$3a = 4 + 11b \quad \Leftrightarrow \quad 3a - 11b = 4. \qquad (*)$$

A occhio (oppure con l'algoritmo di Euclide esteso) si trova che $3 \cdot 4 - 11 \cdot 1 = 1$. Ne segue che $a = 16$ e $b = 4$ soddisfano l'equazione (*) e che $x_0 = 16$ è una soluzione particolare della congruenza (provare per credere).
Conclusione: le soluzioni intere della congruenza sono date da $x = 16 + k11$ al variare di $k \in\ \mathbb{Z}$.
(b) Le soluzioni comprese nell'intervallo $[-5, 20]$ sono 5 (che corrisponde a $k = -1$) e 16 (che corrisponde a $k = 0$).

4. *Calcolare il resto della divisione di 14^{231678} per 11 (giustificare bene i passaggi).*

Dobbiamo innanzitutto calcolare la classe resto $\overline{14^{231678}}$ in $\mathbb{Z}_{11}$. Osserviamo che $\text{mcd}(14, 11) = 1$, dunque la classe resto $\overline{14} = \bar{3}$ appartiene al gruppo $\mathbb{Z}_{11}^*$ delle classi resto modulo 11 che hanno inverso moltiplicativo. $\mathbb{Z}_{11}^*$ è un gruppo abeliano finito di cardinalità 10 e per il Teorema di Lagrange (o Piccolo Teorema di Fermat) vale

$$14^{10} \equiv 3^{10} \equiv 1 \bmod 11.$$

Scrivendo

$$14^{231678} \equiv 3^{231678} \equiv 3^{231670} \cdot 3^8 \equiv 3^{10 \cdot 23167} \cdot 3^8 \equiv 1 \cdot 3^8 \equiv 3^8 \bmod 11.$$

ci siamo ricondotti a calcolare il resto della divisione per 11 di 3^8:

$$3^8 = 3^3 \cdot 3^3 \cdot 3^2 \equiv 5 \cdot 5 \cdot 9 \equiv 3 \cdot 9 \equiv 5 \bmod 11.$$

Conclusione: il resto cercato è 5 (osservare che è un intero fra 0 e 10).

5. *(a) Determinare se $\bar{x} = \overline{35}$ appartiene a $\mathbb{Z}_{100}^*$.*
   (b) Calcolare l'inverso moltiplicativo di $\overline{91}$ in $\mathbb{Z}_{100}^*$.

(a) Poiché $\text{mcd}(35, 100) = 5 > 1$, la classe $\overline{35}$ non appartiene a $\mathbb{Z}_{100}^*$.
(b) In questo caso abbiamo che $\text{mcd}(91, 100) = 1$, dunque $\overline{91}$ ammette inverso moltiplicativo in $\mathbb{Z}_{100}^*$. Dobbiamo determinare una classe resto $\bar{x}$ che soddisfi $\overline{91} \cdot \bar{x} = \bar{1}$ in $\mathbb{Z}_{100}^*$. Ciò equivale a determinare interi x, y tali che

$$91x = 1 + 100y \quad \Leftrightarrow \quad 91x - 100y = 1.$$

Dall'algoritmo di Euclide abbiamo che

$$100 = 91 \cdot 1 + 9, \quad 91 = 9 \cdot 10 + 1,$$

da cui ricaviamo mediante l'algoritmo di Euclide esteso
$1 \cdot 100 + 0 \cdot 91 = 100$
$0 \cdot 100 + 1 \cdot 91 = 91$
$1 \cdot 100 + (-1) \cdot 91 = 9$
$(-10) \cdot 100 + (11) \cdot 91 = 1$
l'inverso cercato

$$\overline{91}^{-1} = \overline{11}.$$

Prova: $\overline{91} \cdot \overline{11} = \overline{1001} = \bar{1} \in \mathbb{Z}_{100}^*$.

6. (a) *Determinare se l'enunciato $\big(\neg A \vee (B \Rightarrow A)\big) \Rightarrow \neg B$ è una contraddizione.*
   (b) Verificare che l'enunciato $A \Rightarrow B$ è logicamente equivalente all'enunciato $\neg A \vee B$.
   (c) Esprimere l'enunciato $\neg\big(\neg B \vee (A \Rightarrow B)\big)$ in forma normale disgiuntiva (somma di prodotti).

(a) Scriviamo la tabella di verità dell'enunciato:

A	B	$B \Rightarrow A$	$\neg A \vee (B \Rightarrow A)$	$\big(\neg A \vee (B \Rightarrow A)\big) \Rightarrow \neg B$
V	V	V	V	F
V	F	V	V	V
F	V	F	V	F
F	F	V	V	V

Conclusione: l'enunciato non è una contraddizione, in quanto non è falso per ogni valore di verità di A e B.
(b) Vedi soluzioni Esercizi 8 (2008-2009), n.2(e).
(c) Per il punto (b), l'enunciato $\neg\big(\neg B \vee (A \Rightarrow B)\big)$ è logicamente equivalente a $\neg\big(\neg B \vee (\neg A \vee B)\big)$. Per l'associatività e le formule di De Morgan, abbiamo

$$\neg\big(\neg B \vee (\neg A \vee B)\big) \Leftrightarrow \neg\big(\neg B \vee \neg A \vee B\big) \Leftrightarrow B \wedge A \wedge \neg B.$$

Quest'ultimo enunciato è logicamente equivalente a una contraddizione, in quanto già $B \wedge \neg B$ lo è.