ALGEBRA E LOGICA (Geatti) 3° appello Roma, 16 luglio 2009, ore 10–12.

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.(a) *Determinare tutte le soluzioni intere del sistema di congruenze* $\begin{cases} x \equiv 2 \bmod 4 \\ x \equiv 4 \bmod 6. \end{cases}$

.(b) *Determinare le soluzioni del sistema comprese nell'intervallo* $[-20, 20]$.

Sol. (a) Il sistema dato ha soluzioni in quanto il massimo comun divisore $mcd(4,6) = 2$ divide $4 - 2 = 2$. Lo risolviamo per sostituzione.
Dalla prima congruenza ricaviamo $x = 2 + 4k, \quad k \in \mathbb{Z}$. Sostituiamo questa relazione nella seconda congruenza:

$$2 + 4k \equiv 4 \bmod 6 \quad \Leftrightarrow \quad 2 + 4k = 4 + 6h \quad \Leftrightarrow \quad 4k - 6h = 2, \quad k, h \in \mathbb{Z} \qquad (*)$$

$$\Leftrightarrow \quad 2k - 3h = 1, \quad k, h \in \mathbb{Z}. \qquad (**)$$

Una soluzione particolare dell'equazione diofantea (**) è data da $(k, h) = (-4, -3)$. Poiché $mcd(2, 3) = 1$, la soluzione generale è data da $(k, h) = (-4, -3) + (3M, 2M), \quad M \in \mathbb{Z}$.
ATTENZIONE: abbiamo sfruttato il fatto che $mcd(2, 3) = 1$! Dunque è importante semplificare da (*) a (**).
Sostituendo $k = -4 + 3M$ nella relazione iniziale $x = 2 + 4k$, troviamo le soluzioni cercate

$$x = 2 + 4(-4 + 3M) = -14 + 12M = 10 + 12M, \quad M \in \mathbb{Z}.$$

(b) Le soluzioni comprese nell'intervallo $[-20, 20]$ sono:

$$x = -14, -2, 10$$

e corrispondono rispettivamente ai valori $M = -2$, $M = -1$, $M = 0$.

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

Sol. Siccome A ha 3 elementi, l'insieme $\mathcal{P}(A)$ 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 biiezione fra essi. Infatti ne esistono tante (32320 per essere precisi). Eccone un esempio: la biezione g definita da

$g(\emptyset) = (0, 1)$,
$g(\{0\}) = (0, 2)$,
$g(\{1\}) = (1, 0)$,
$g(\{0, 1\}) = (1, 1)$,
$g(\{2\}) = (1, 2)$,
$g(\{0, 2\}) = (2, 0)$,
$g(\{1, 2\}) = (2, 1)$,
$g(A) = (2, 2)$.

3. *Sia* p *un numero primo e sia* $\mathbb{Z}_p^*$ *il gruppo delle classi resto modulo* p *che hanno inverso moltiplicativo.*
   (a) Quanti elementi ha Z_p^**? (spiegare bene la risposta).*
   (b) Enunciare il Teorema di Lagrange (o Piccolo Teorema di Fermat) per $\mathbb{Z}_p^*$.
   (c) Sia $p = 19$. *Calcolare* $\overline{25}^{1338}$ *modulo 19.*

Sol. (a) Il gruppo $\mathbb{Z}_p^*$ è costituito dalle classi $\bar{x}$ con $mcd(x, p) = 1$. Se p è primo, tutte le classi $\bar{x} \neq \bar{0}$ soddisfano $mcd(x, p) = 1$, per cui la cardinalità di $\mathbb{Z}_p^*$ è $p - 1$.

(b) Vale $\quad x^{p-1} \equiv 1 \mod p, \quad$ per ogni intero x che soddisfa $mcd(x,p) = 1$. In altre parole, per ogni $\bar{x} \in \mathbb{Z}_p^*$ vale $\bar{x}^{p-1} = \bar{1}$ in $\mathbb{Z}_p^*$.

(c) Poiché 19 è primo, $\mathbb{Z}_{19}^*$ ha cardinalità 18 e vale $\quad \bar{x}^{18} \equiv \bar{1} \mod 19, \quad$ per ogni intero x che soddisfa $mcd(x,19) = 1$. Calcolando modulo 19, abbiamo

$$\overline{25}^{1338} \equiv \bar{6}^{1338} \equiv \bar{6}^{74\cdot18+6} \equiv \bar{6}^{74\cdot18} \cdot \bar{6}^6 \equiv \bar{1} \cdot \bar{6}^6 \equiv \overline{11}.$$

4. *Sia $n = 354$.*
   (a) Determinare se $\overline{12}$ appartiene a $\mathbb{Z}_n^*$ (spiegare).
   (b) Verificare che $\overline{53}$ appartiene a $\mathbb{Z}_n^*$ (spiegare).
   (c) Calcolare l'inverso di $\overline{53}$ in $\mathbb{Z}_n^*$.

Sol. (a) Poiché $mcd(12,354) = 6 \neq 1$, si ha che $\overline{12}$ NON appartiene a $\mathbb{Z}_{354}^*$.

(b) Per verificare che $\overline{53}$ appartiene a $\mathbb{Z}_{354}^*$, osserviamo che 53 è un numero primo da cui segue immediatamente che $mcd(53,354) = 1$.

(c) L'inverso di $\overline{53}$ in $\mathbb{Z}_{354}^*$ è per definizione un $\bar{x} \in \mathbb{Z}_{354}^*$ che soddisfa

$$\overline{53} \cdot \bar{x} \equiv \bar{1} \mod 354 \quad \Leftrightarrow \quad \exists y \in \mathbb{Z}: \quad 53x + 354y = 1. \tag{$*$}$$

Per determinare una soluzione particolare dell'equazione diofantea (*) applichiamo l'algoritmo di Euclide "esteso":

$$354 = 6 \cdot 53 + 36, \quad 53 = 1 \cdot 36 + 17, \quad 36 = 2 \cdot 17 + 2, \quad 17 = 8 \cdot 2 + 1,$$

da cui

$1 \cdot 354 + 0 \cdot 53 = 354$
$0 \cdot 354 + 1 \cdot 53 = 53$
$1 \cdot 354 + (-6) \cdot 53 = 36$
$(-1) \cdot 354 + 7 \cdot 53 = 17$
$3 \cdot 354 + (-20) \cdot 53 = 2$
$-25 \cdot 354 + 167 \cdot 53 = 1.$

Questo calcolo ci conferma che $mcd(53,354) = 1$ e ci fornisce l'inverso cercato $\bar{x} = \overline{167}$.
Prova: $\overline{53} \cdot \overline{167} \equiv \bar{1} \mod 354$.

5. *In un'algebra di Boole $(A, +, \cdot, ')$ siano date le espressioni Booleane*
   $$E: \ xyz' + xy'z + x'y \qquad\qquad F: \ xz' + xy'z + x'yz'.$$
   (a) Determinare se E ed F sono equivalenti;
   (b) Scrivere F come somma di implicanti primi;
   (c) Scrivere F in forma minimale.

Sol. (a) Completando le espressioni otteniamo

$$E: \ xyz' + xy'z + x'yz + x'yz', \qquad F: \ xyz' + xy'z' + xy'z + x'yz'.$$

Poiché la forma completa è unica, è evidente che E ed F non sono equivalenti.

(b) Applichiamo ad F il metodo del consenso:
$F = xz' + xy'z + x'yz' \quad + \quad xy' = xz' + x'yz' + xy' =$ (il consenso di xz' e $xy'z$ è $x^2y' = xy'$)
$= xz' + x'yz' + xy' \quad + \quad yz' = xz' + xy' + yz'$. (il consenso di xz' e $x'yz'$ è $y(z')^2 = yz'$)
A questo punto ci fermiamo perché l'unico consenso rimasto, cioè quello di xy' e yz' che è uguale a xz', è un termine che esiste gia' in F). Conclusione: $F = xz' + xy' + yz'$ è somma di implicanti primi.

(c) Per scrivere F in forma minimale la ricompletiamo e controlliamo se uno dei completamenti di xz', xy', yz' è ripetuto. In tal caso lo eliminiamo ottenendo così una forma più compatta di F:

$$F = xyz' + xy'z' \quad + \quad xyz' + x'yz' \quad + \quad xy'z + xy'z'.$$

Non ci sono ripetizioni, e dunque $F = xz' + xy' + yz'$ è anche una forma minimale di F.

6. *Si consideri il reticolo* (D_{18}, mcd, mcm) *(qui* D_{18} *indica l'insieme dei divisori di 18).*
   (a) *Qual è la relazione di ordine parziale "* $\leq$ *" indotta su* D_{18} *dalle operazioni di reticolo? Disegnare il diagramma di Hasse associato. Determinare* $A = \{x \in D_{18} \mid x\text{“} \leq \text{”}6\}$ *e indicarlo nella figura.*
   (b) *Determinare tutti i maggioranti e tutti i minoranti di* A *in* D_{18}*. Dire se* A *ha massimo o minimo (spiegare).*
   (c) *Per ogni elemento di* D_{18} *esibire un eventuale complemento e dire se è unico (spiegare).*

Sol. (a) Poiché $18 = 2 \cdot 3^2$, l'insieme dei divisori di 18 è dato

$$D_{18} = \{1, 2, 3, 6, 9, 18\}.$$

Siano $a, b \in D_{18}$. La relazione di ordine parziale " $\leq$ " indotta su D_{18} dalle operazioni di reticolo è:

$$a\text{“} \leq \text{”}b \text{ se } mcd(a, b) = a, \quad \text{ossia se } a \text{ divide } b. \qquad (*)$$

Il diagramma di Hasse associato è dato da

....

Si ha che $A = \{1, 2, 3, 6\}$. I maggioranti di A in D_{18} sono 6 e 18: sono divisi da tutti gli elementi di A, dunque sono "maggiori o uguali" di tutti gli elementi di A secondo l'ordinamento parziale (*). Notare che invece 9 non è un maggiorante di A: l'elemento 2 appartiene ad A ma non divide 9. Perciò 2 non è maggiorato da 9 (non è nemmeno confrontabile con 9). L'elemento $6 \in A$ è massimo di A. L'elemento $1 \in A$ è minorante di A in D_{18} e minimo.

(c) L'unico elemento di D_{18} ad avere complemento è 2. Il suo complemento è 9: infatti $mcd(2, 9) = 1$ e $mcm(2, 9) = 18$. Tale complemento è unico. Si verifica facilmente che per $a \in D_{18}$ vale $mcm(2, a) = 19$ se e solo se $a = 9$.