ALGEBRA E LOGICA (Geatti) 2° appello Roma, 28 febbraio 2012, ore 11-13.

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

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

1. Siano dati i sistemi di congruenze $\begin{cases} x \equiv 5 \mod 6 \\ x \equiv 3 \mod 4 \end{cases}$ e $\begin{cases} 2x \equiv 5 \mod 6 \\ x \equiv 3 \mod 4. \end{cases}$
   (i) Determinare quale dei due ha soluzioni intere, spiegando la risposta.
   (ii) Determinare tutte le soluzioni intere di tale sistema.

*Sol.* Sistema 2: $mcd(2,6) = 2$ e 2 non divide 5. Ne segue che la prima congruenza del sistema, e a maggior ragione il sistema, non hanno suluzioni intere.

Sistema 1: in questo caso è evidente che le congruenze del sistema hanno singolarmente soluzioni intere (sono già nella forma $x \equiv x_0 \mod n$). Questo di per sè non garantisce che il sistema abbia soluzioni intere. In questo caso, poiché $mcd(4,6)$ divide 4-6=-2, il sistema ha soluzioni intere. (In alternativa uno può comunque procedere per sostituzione e vedere cosa succede). Le soluzioni della prima congruenza sono gli interi $x = 5 + 6k,\ k \in \mathbb{Z}$. Sostituendo nella seconda congruenza otteniamo una equazione a coefficienti interi

$$6k - 4h = -2 \quad \Leftrightarrow \quad 3k - 2h = -1, \qquad (*)$$

con soluzione generale $(k,h) = (-1 + 2M, -1 + 3M),\ M \in \mathbb{Z}$.
ATTENZIONE: senza la semplificazione di coefficienti in (*) si perdono metà soluzioni dell'omogenea associata e quindi dell'equazione completa!!!!
Dall'espressione di $k = -1 + 2M,\ M \in \mathbb{Z}$, otteniamo la soluzione generale del sistema

$$x = 5 + 6k = 5 + 6(-1 + 2M) = -1 + 12M = 11 + 12M, \quad M \in \mathbb{Z}.$$

2. Sia $R$ la relazione su $\mathbb{Z}$ data da $xRy$ se $x + y$ è pari. Sia $X = \{1,2,3,4,5,6,7,8\}$.
   (a) Dimostrare che $R$ è una relazione di equivalenza.
   (b) Determinare le classi di equivalenza di $R$ su $X$.
   (c) Sia $R$ la relazione su $X$ data da $xRy$ se $x + y$ è dispari. Determinare se $R$ è o meno una relazione di equivalenza (giustificare).

*Sol.* (a) $R$ è riflessiva: $\forall x \in \mathbb{Z}$ vale $x + x = 2x$ pari;
$R$ è simmetrica: $\forall x, y \in \mathbb{Z}$, se $x + y$ è pari, allora anche $y + x = x + y$ è pari;
$R$ è transitiva: $\forall x, y, z \in \mathbb{Z}$, se $x + y$ è pari, cioè $x + y = 2k,\ k \in \mathbb{Z}$ e $y + z$ è pari, cioè $y + z = 2h,\ h \in \mathbb{Z}$, allora $x + z = 2k + 2h - 2y$ è pari.

(b) Si può anche osservare che la somma di due interi è pari se e solo se sono entrambi pari o entrambi dispari, etc... Da questa osservazione segue che due elementi di $X$ sono equivalenti se e solo se hanno la stessa parità. In particolare ci sono due classi di equivalenza, che determinano una partizione di $X$, date da

$$\{1,3,5,7\}, \{2,4,6,8\}.$$

(c) $\forall x \in \mathbb{Z}$ vale $x + x = 2x$ pari; dunque la relazione $xRy$ se $x + y$ è dispari non è riflessiva. In particolare non può essere una relazione di equivalenza.

3. Il signor Rossi desidera ricevere messaggi criptati e decide di adottare il criptosistema RSA.
   (a) Preparargli un kit di chiavi pubbliche $N$, $E$ e chiave segreta $D$, con $N = 77$ ed $E = 11$.
   (b) Spedire all'utente Verdi, con chiavi pubbliche $N = 77$ ed $E = 7$, il messaggio $m = 13$ dopo averlo criptato (impostare il calcolo).
   (c) L'utente Verdi con chiavi pubbliche $N = 77$, $E = 19$ e chiave segreta $D = 53$ riceve il messaggio criptato $mc = 50$. Come lo decifra?(impostare il calcolo).

*Sol.* (a) $N = 7 * 11$, $p = 7$, $q = 11$: la chiave segreta è data da $D = E^{-1} \bmod (p-1)(q-1)$, cioè $D = 11^{-1} \bmod 60$. Risolviamo dunque l'equazione

$$11x \equiv 1 \bmod 60 \quad \Leftrightarrow \quad 11x = 1 + 60y, \quad x, y \in \mathbb{Z}.$$

Da $mcd(11, 60) = 1$, due passaggi dell'algoritmo di Euclide esteso danno $D = 11$. Prova: $11 * 11 = 121 \equiv 1 \bmod 60$.

(b) Il messaggio $m = 13$ criptato sarà $mc = 13^7 \bmod 77$.

(c) Il messaggio $mc = 50$ decriptato sarà $m = 50^{53} \bmod 77$.

4. Sia $D_{12}$ l'insieme dei divisori di 12, con l'ordinamento dato dalla divisibilità: $m \text{“} \leq \text{”} n$ se $m|n$.
   (a) Disegnare il diagramma di Hasse associato.
   (b) Determinare l'insieme dei maggioranti di 4 e l'insieme dei minoranti di 4 in $D_{12}$.
   (c) Richiamare la definizione di *complemento* di un elemento $m \in D_{12}$.
   (d) Per ogni elemento di $D_{12}$, determinare se ammette o meno complemento e se tale complemento è unico (giustificare bene le risposte).

*Sol.* $12 = 2^2 \cdot 3$ e $D_{12} = \{1, 2, 3, 4, 6, 12\}$.

(b) $magg(4) = \{m \in D_{12} \mid 4 \text{ divide } m\} = \{4, 12\}$;
$min(4) = \{m \in D_{12} \mid m \text{ divide } 4\} = \{1, 2, 4\}$.

(c) $D_{12}$ è un reticolo limitato con max=12 e min=1. Sia $m \in D_{12}$. Un complemento di $m$ in $D_{12}$ è un intero $\bar{m} \in D_{12}$ tale che $mcd(m, \bar{m}) = 1$ e $mcm(m, \bar{m}) = 12$. Poiché $D_{12}$ è un reticolo distributivo, se esiste $\bar{m}$ è anche unico.

(d) Vediamo subito che $\bar{1} = 12$ e $\overline{12} = 1$ e che $\bar{3} = 4$ e $\bar{4} = 3$. Invece 2 e 6 non ammettono complemento: basta provare....

5. Enunciare il Piccolo Teorema di Fermat. Usare il Piccolo Teorema di Fermat per verificare che $n = 15$ non è primo.

*Sol.* PTF: Sia $p \in \mathbb{Z}$ primo. Allora per ogni $x \in \mathbb{Z}$, con $mcd(x, p) = 1$, vale $x^{p-1} \equiv 1 \bmod p$.
Prendiamo $x = 2$. Abbiamo che $mcd(2, 15) = 1$, ma al tempo stesso

$$2^{14} = 2^4 \cdot 2^4 \cdot 2^4 \cdot 2^2 \equiv 4 \not\equiv 1 \bmod 15.$$

Ne segue che 15 non è primo.

6. In un'algebra di Boole $(A, +, \cdot, ')$ siano data l'espressione Booleana
$$E: \ x'z + xyz + yz \qquad F: \ xyz + xy' + x'y'z.$$
   (a) Determinare se $E$ ed $F$ sono equivalenti;
   (b) Scrivere $F$ come somma di tutti gli implicanti primi;
   (c) Scrivere $F$ in forma minimale.

*Sol.* (a) Per poter confrontare due espressioni booleane bisogna portarle in una forma “unica”, cioè la somma di prodotti completa oppure la somma di tutti gli implicanti primi. Optiamo per la seconda, così rispondiamo anche alla domanda (b).
Usando distributività e assorbimento, troviamo

$$E = x'z + xyz + yz = x'z + xy(z + 1) = x'z + yz.$$

Poiché il metodo del consenso non ha passi non banali, $x'z + yz$ è l'espressione di $E$ come somma di tutti gli implicanti primi. Applicando il consenso ai primi due termini e semplificando con l'assorbimento, troviamo

$$F = xyz + xy' + x'y'z = xyz + xy' + x'y'z + xz = xy' + x'y'z + xz.$$

Applicando il consenso ai primi due termini e semplificando con l'assorbimento, troviamo

$$F = xy' + x'y'z + xz = xy' + x'y'z + xz + y'z = xy' + xz + y'z.$$

Poiché il metodo del consenso non ha passi non banali, $xy' + xz + y'z$ è l'espressione di $F$ come somma di tutti gli implicanti primi. È evidente che $E \neq F$.

(c) Completando i monomi di $F$ , troviamo

$$(xy'z + xy'z') + (xyz + xy'z) + (xy'z + x'y'z).$$

Poiché nessun implicante primo è contenuto nella somma degli altri due, $xy' + xz + y'z$ è anche una forma minimale di $F$. In questo caso è unica.