ALGEBRA E LOGICA (Geatti) 2° appello Roma, 17 febbraio 2009, ore 9,30 – 11,30.

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. *Determinare tutte le soluzioni intere della congruenza* $2x \equiv 5 \bmod 15$. *Determinare tutte le soluzioni della congruenza comprese nell'intervallo* $[-5, 25]$.

Sol. Poiché il massimo comun divisore $mcd(2, 15) = 1$ divide 5, la congruenza ammette soluzioni intere. Esse saranno della forma $x = x_0 + 15K$, dove x_0 è una soluzione particolare e K varia fra gli interi. Una soluzione particolare si trova a partire da una soluzione particolare dell'equazione diofantea associata $2x + 15K = 5$, quale ad esempio $(x_0, K_0) = (-5, 1)$. Dunque la soluzione generale della congruenza è data da

$$x = -5 + 15K \equiv 10 + 15K, \quad K \in \mathbb{Z}.$$

Fra le soluzioni $x = 10+15K$, $K \in \mathbb{Z}$, quelle comprese nell'intervallo $[-5, 25]$ sono $-5, 10, 25$, e corrispondono rispettivamente a $K = -1, 0, 1$.

2. *Sia data la funzione definita per ricorrenza mediante:* $F(0) = 0$, $F(n) = n + F(n-1)$, $n \geq 1$.
   (a) Calcolare $F(1)$, $F(2), \ldots, F(5)$;
   (b) Per induzione verificare che $F(n) = \frac{n(n+1)}{2}$.

Sol. (a) $F(1) = 1 + F(0) = 1$, $F(2) = 2 + F(1) = 3$, $F(3) = 3 + F(2) = 6$,
$F(4) = 4 + F(3) = 10$, $F(5) = 5 + F(4) = 15$.
(b) Vedi Esercizi 1, n. 26.

3. *Sia* R *la relazione su* $\mathbb{Z}_7$ *definita da: "*x R y *se e soltanto se* $x^2 \equiv y^2 \pmod 7$*".*
   (a) Dimostrare che R *è una relazione di equivalenza.*
   (b) Determinare le classi di equivalenza.

Sol. (a) Verifichiamo che la relazione R è riflessiva, simmetrica e transitiva. Tutte e tre queste proprietà seguono direttamente dal fatto che la congruenza fra interi modulo 7 è riflessiva, simmetrica e transitiva e dunque rimane tale sui quadrati modulo 7.
R è riflessiva: $x^2 \equiv x^2 \bmod 7$;
R è simmetrica: $x^2 \equiv y^2 \bmod 7$ implica $y^2 \equiv x^2 \bmod 7$;
R è transitiva: $x^2 \equiv y^2 \bmod 7$ e $y^2 \equiv z^2 \bmod 7$ implica $x^2 \equiv z^2 \bmod 7$.
(b) Calcoliamo $\bar{x}^2$, al variare di $\bar{x} \in \mathbb{Z}_7$:

$$\bar{0}^2 = \bar{0}, \quad \bar{1}^2 = \bar{1}, \quad \bar{2}^2 = \bar{4}, \quad \bar{3}^2 = \bar{2}, \quad \bar{4}^2 = \bar{2}, \quad \bar{5}^2 = \bar{4}, \quad \bar{6}^2 = \bar{1}.$$

Le classi di equivalenza di $\mathbb{Z}_7$ rispetto ad R sono 4 e individuano una partizione di $\mathbb{Z}_7$. Ogni classe di equivalenza contiene tutte e sole le classi resto che hanno lo stesso quadrato modulo 7:

$$\{\bar{0}\}, \quad \{\bar{1}, \bar{6}\}, \quad \{\bar{2}, \bar{5}\}, \quad \{\bar{3}, \bar{4}\}.$$

4. *Sia* $n = 91 = 7 \cdot 13$.
   (a) Verificare che $\bar{5}$ *appartiene a* $\mathbb{Z}_{91}^*$.
   (b) Calcolare $\bar{5}^{14} \bmod 91$.

Sol. (a) Poiché $mcd(5, 91) = 1$, si ha che $\bar{5}$ appartiene a $\mathbb{Z}_{91}^*$.
(b) Sia $\bar{x} \equiv \bar{5}^{14} \bmod 91$. Questo equivale a

$$\begin{cases} \bar{x} \equiv \bar{5}^{14} \bmod 7 \\ \bar{x} \equiv \bar{5}^{14} \bmod 13. \end{cases} \qquad (*)$$

Poiché 7 e 13 sono primi, per il Piccolo Teorema di Fermat si ha che $\bar{5}^6 \equiv \bar{1} \mod 7$ e $\bar{5}^{12} \equiv \bar{1} \mod 13$. In particolare, il sistema (*) equivale a

$$\begin{cases} \bar{x} \equiv \bar{5}^2 \mod 7 \\ \bar{x} \equiv \bar{5}^2 \mod 13 \end{cases}$$

ed alla congruenza $\bar{x} \equiv 25 \mod 91$. Conclusione: $\bar{5}^{14} \equiv \overline{25} \mod 91$.

5. *In un'algebra di Boole* $(A, +, \cdot, ')$ *sia data l'espressione Booleana*
$$E: \quad xyz + xy'z + xyz' + xy'z' + x'y'z'.$$
   (a) Scrivere E *come somma di implicanti primi;*
   (b) Determinare una forma minimale di E*.*

Sol. (a) $E: \quad xyz+xy'z+xyz'+xy'z'+x'y'z' = xyz+xy'z+xyz'+(x+x')y'z' = xyz+xy'z+xyz'+y'z'$.
Sommiamo ad E il consenso fra i primi due termini e semplifichiamo:
$xyz + xy'z + xyz' + y'z' \ + \ xz = xz + xyz' + y'z'$.
Sommiamo ad E il consenso fra gli ultimi due termini e semplifichiamo:
$xz + xyz' + y'z' \ + \ xz' = x(z + z') + xyz' + y'z' = x + xyz' + y'z' = x(1 + yz') + y'z' = x + y'z'$.
Conclusione: E come somma di implicanti primi è dato da: $x + y'z'$.

(b) Se portiamo $x + y'z'$ in forma completa, troviamo

$$x(y + y')(z + z') \ + \ (x + x')y'z' \ = \ xyz + xyz' + xy'z + xy'z' \quad + \quad xy'z' + x'y'z'.$$

È evidente che i due implicanti primi di E sono distinti e nessuno dei due può essere eliminato. Quindi l'espressione $x + y'z'$ è anche minimale.

6. *Nell'algebra di Boole* $(P, \wedge, \vee, \neg)$ *considerare le espressioni booleane*
$$E: \quad \neg\big((A \wedge B) \bigvee \neg(A \vee B)\big) \qquad F: \quad \neg\big((A \vee B) \bigvee \neg(\neg A \vee \neg B)\big).$$
   (a) Portare E *ed* F *in forma normale disgiuntiva (cioè come somma di prodotti).*
   (b) Determinare se E *implica* F*.*

Sol. (a) $E: \quad \neg\big((A \wedge B) \bigvee \neg(A \vee B)\big) = \neg(A \wedge B) \bigwedge (A \vee B) = (\neg A \vee \neg B) \bigwedge (A \vee B) =$
$\neg A \wedge A \bigvee \neg A \wedge B \bigvee \neg B \wedge A \bigvee \neg B \wedge B = \neg A \wedge B \bigvee \neg B \wedge A.$

$F: \quad \neg\big((A \vee B) \bigvee \neg(\neg A \vee \neg B)\big) = \neg(A \vee B) \bigwedge (\neg A \vee \neg B) = (\neg A \wedge \neg B) \bigwedge (\neg A \vee \neg B) =$
$= \neg A \wedge \neg B \wedge \neg A \bigvee \neg A \wedge \neg B \wedge \neg B = \neg A \wedge \neg B \bigvee \neg A \wedge \neg B = \neg A \wedge \neg B.$

(b) Abbiamo che E implica F se ogni volta che E è vera anche F è vera. Nel nostro caso questo non succede. Ad esempio, se A è vera e B è falsa, abbiamo che E è vera, ma F è falsa. Dunque E non implica F.