Algebra e Logica (Schoof) 2^o appello 15 febbraio 2018, ore 10:00–12:00.

COGNOME ..... *NOME* .....

Risolvere gli esercizi negli spazi predisposti. Accompagnare le risposte con spiegazioni *chiare ed essenziali.* Consegnare SOLO QUESTO FOGLIO. Ogni esercizio vale 5 punti.

Ci sono quattro versioni leggermente diverse. Eccone una.

1. Sia n un intero che, scritto in base 7, è dato da $n = 123$. Scrivere n in base 6.
2. Scrivere la forma normale disgiuntiva del polinomio Booleano nelle variabili x, y, z dato da $x \vee y\overline{z}$.
3. (a) Sia n il quadrato di un numero primo dispari. Quanti sono gli elementi $\overline{x} \in \mathbf{Z}_n^*$ con $\overline{x}^2 = \overline{1}$?
   (b) Sia n il prodotto di due primi dispari distinti. Quanti sono gli elementi $\overline{x} \in \mathbf{Z}_n^*$ con $\overline{x}^2 = \overline{1}$?
4. Sia dato l'insieme $X = \{2, 4, 6, 9, 12, 18, 27, 36, 48, 60, 72\}$, ordinato mediante $d \leq d'$ quando d divide d'.
   (a) Determinarne gli elementi massimali e minimali.
   (b) Esibirne, se esistono, i massimi e minimi assoluti.
   (c) Trovare i maggioranti di $\{2, 9\}$ e, se esiste, $\sup(2, 9)$.
5. Per ricevere messaggi criptati, la banca adotta il criptosistema RSA con chiavi pubbliche il modulo N e l'esponente E, e chiave segreta D.
   (a) Determinare E, sapendo che $N = 77$ e $D = 13$.
   Nelle domande (b) e (c) non è necessario svolgere i calcoli.
   (b) La banca riceve il messaggio criptato $m = 19$. Che cosa calcola per decriptarlo?
   (c) Che cosa si calcola per criptare il messaggio $m = 23$ da inviare alla banca?
6. Dire se le seguenti affermazioni sono vere o false. Spiegare perché.
   (a) $\forall x \in \mathbf{R}\, \forall y \in \mathbf{R}\, \exists z \in \mathbf{R} : xy = z$;
   (b) $\exists x \in \mathbf{R}\, \forall y \in \mathbf{R}\, \forall z \in \mathbf{R} : xy = z$;
   (c) $\exists x \in \mathbf{R}\, \exists y \in \mathbf{R}\, \forall z \in \mathbf{R} : xy = z$.

Soluzioni.

1. In base 10 abbiamo che $n = 7^2 + 2 \cdot 7 + 3 = 66 = 6^2 + 5 \cdot 6 + 0$. In base 6 abbiamo quindi che $n = 150$.
2. $xyz \vee x\overline{y}z \vee xy\overline{z} \vee x\overline{y}\,\overline{z} \vee \overline{x}y\overline{z}$.
3. Questo è l'esercizio 6 del foglio 5.
4. Questo è l'esercizio 2 del foglio 8.
5. Si ha che $N = 7 \cdot 11$ e $\phi(N) = 6 \cdot 10 = 60$. L'esponente E è determinato dalla congruenza $DE \equiv 1 \pmod{\phi(N)}$, cioè da $13E \equiv 1 \pmod{60}$. Usando l'algoritmo euclideo, si trova che $E = 37$.
   (b) La banca calcola $m^D = 19^{13} \pmod{77}$. (c) Si invia $m^E = 23^{37} \pmod{77}$ alla banca.
6. L'affermazione (a) è vera. Per ogni $x, y \in \mathbf{R}$ possiamo prendere $z = xy$. L'affermazione (b) è falsa. Se esistesse x, allora x sarebbe uguale a z/y per ogni y, z. Questo è assurdo. Anche l'affermazione (c) è falsa. Se fosse $xy = z$ per ogni z, allora varrebbero $xy = 0$, ma anche $xy = 1$. Assurdo.