Algebra e Logica (Schoof) 4^o appello 18 luglio 2018, ore 11:00–13:00.

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.

1. Determinare tutte le soluzioni $x \in \mathbf{Z}$ del sistema
$$\begin{cases} 3x \equiv 6 \pmod 9, \\ 9x \equiv 3 \pmod 6. \end{cases}$$

2. Sia dato il polinomio Booleano $x\overline{y}z \vee xy\overline{z} \vee \overline{x}\,\overline{y}\,\overline{z}$ in tre variabili x, y e z. Scriverlo come somma di tutti gli implicanti primi e determinare una sua forma minimale.

3. Determinare $a, b \in \mathbf{Z}$ tali che $101a + 103b = \mathrm{mcd}(101, 103)$.

4. 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 D, sapendo che $N = 85$ e $E = 43$.
   Nelle domande (b) e (c) non è necessario svolgere i calcoli.
   (b) La banca riceve il messaggio criptato $m = 11$. Che cosa calcola per decriptarlo?
   (c) Che cosa si calcola per criptare il messaggio $m = 34$ da inviare alla banca?

5. Sia $X = \mathbf{Z}_{15}^*$. Definiamo una relazione R su $\mathbf{Z}_{15}^*$ come segue: per due elementi $\overline{x}, \overline{y} \in \mathbf{Z}_{15}^*$ si ha che $\overline{x}\,R\,\overline{y}$, quando esiste $\overline{z} \in \mathbf{Z}_{15}^*$ tale che $\overline{x}\,\overline{y} = \overline{z}^2$
   (a) Dimostrare che si tratta di una relazione di equivalenza.
   (b) Quanti classi di equivalenza ci sono?

6. Dire se le seguenti affermazioni sono vere o false. Spiegare perché.
   (a) $\forall x \in \mathbf{R}\, \forall y \in \mathbf{R}\, \forall z \in \mathbf{R} : xy = z$;
   (b) $\exists x \in \mathbf{R}\, \forall y \in \mathbf{R}\, \exists z \in \mathbf{R} : xy = z$;
   (c) $\exists x \in \mathbf{R}\, \exists y \in \mathbf{R}\, \forall z \in \mathbf{R} : xy = z$;
   (d) $\forall x \in \mathbf{R}\, \exists y \in \mathbf{R}\, \exists z \in \mathbf{R} : xy = z$.

Soluzioni.

1. Il sistema è equivalente al sistema
$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 1 \pmod 2, \end{cases}$$
   con soluzione $x \equiv 5 \pmod 6$.
2. Questo è l'esercizio 2 del foglio 11.
3. Questo è l'eserczio 4 del foglio 4.
4. (a) Si ha che $N = pq$ con $p = 5$ e $q = 17$. La congruenza $ED \equiv 1 \pmod{(p-1)(q-1)}$ diventa $ED = 43D \equiv 1 \pmod{64}$ e quindi $D \equiv 3 \pmod{64}$. (b) La banca calcola $11^{43} \pmod{85}$. (c) Si calcola $34^3 \pmod{85}$.
5. Ci sono quattro classi di equivalenza: $\{\overline{1}, \overline{4}\}$, $\{\overline{2}, \overline{8}\}$, $\{\overline{11}, \overline{14}\}$ e $\{\overline{7}, \overline{13}\}$.
6. (a) Non è vera. (b) È vera. Infatti, possiamo prendere $x = 1$. Allora per ogni $y \in \mathbf{R}$ esiste z con $y = z$, perché prendiamo $z = y$. (c) È falsa. (d) È vera. Infatti, dato $x \in \mathbf{R}$, possiamo prendere $y = 1$ e $z = x$.