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

Inserire le risposte negli spazi predisposti, *accompagnandole con spiegazioni* chiare ed essenziali. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 7.5 punti.

1. Sia $\mathbf{N}$ l'insieme dei numeri naturali e sia $A = \{1, 4, 9, \ldots\}$ l'insieme dei quadrati di elementi di $\mathbf{N}$.
   (a) Costruire una funzione $A \longrightarrow \mathbf{N}$ suriettiva.
   (b) Costruire un'iniezione $\mathbf{N} \longrightarrow A$ che *non* è una biezione.

Notiamo prima che esistono *infinite* funzioni che hanno le proprietà richieste.

(a) Sia $f : A \longrightarrow \mathbf{N}$ la funzione definita da $f(x) = \sqrt{x}$. Allora f è suriettiva, poiché per ogni $n \in \mathbf{N}$ esiste $x \in A$ (vale a dire $x = n^2$) con $f(x) = n$.

(b) Sia $g : \mathbf{N} \longrightarrow A$ la funzione definita da $g(n) = (n+1)^2$. Allora g è iniettiva. Infatti, se $g(n) = g(m)$, allora $(n+1)^2 = (m+1)^2$ e quindi $m = n$. Ma g non è suriettiva, poiché non esiste $n \in \mathbf{N}$ per cui $g(n) = (n+1)^2$ è uguale ad $1 \in A$.

2. Si consideri il sistema crittografico RSA corrispondente al modulo $n = 143 = 11 \cdot 13$ e all'esponente $D = 47$.
   (a) Cifrare il messaggio "17", cioè calcolare il resto della divisione per 143 del numero 17^{47} (suggerimento: calcolare il resto delle divisioni per 11 e per 13 del numero 17^{47});
   (b) Determinare un esponente E che consenta di decifrare il messaggio precedente. In altre parole: determinare un numero naturale E tale che $(17^{47})^E \equiv 17 \pmod{143}$.

(a) Siccome $47 \equiv 7 \pmod{10}$, abbiamo, per il Teorema di Fermat, che $x = 17^{47} \equiv 6^7 = 36^3 \cdot 6 \equiv 3^3 \cdot 6 = 27 \cdot 6 \equiv 5 \cdot 6 \equiv 8 \pmod{11}$. Similmente, $47 \equiv -1 \pmod{12}$ e quindi $x = 17^{47} \equiv 4^{-1} \pmod{13}$. Usando l'algoritmo euclideo si calcola che l'inverso moltiplicativo di 4 (mod 13) è uguale a 10. Abbiamo quindi che $17^{47} \equiv 10 \pmod{13}$. Con il Teorema Cinese del resto si trova che $x \equiv 140 \pmod{143}$.

(b) Ogni soluzione $E \in \mathbf{N}$ della congruenza $E \cdot 47 \equiv 1 \pmod{10 \cdot 12}$ fornisce un possibile esponente. Per trovare una soluzione, si applica l'algoritmo Euclideo:

$$\begin{aligned}
1 \cdot 120 + \ 0 \cdot 47 &= 120, \\
0 \cdot 120 + \ 1 \cdot 47 &= 47, \\
1 \cdot 120 - \ 2 \cdot 47 &= 26, \\
-1 \cdot 120 + \ 3 \cdot 47 &= 21, \\
2 \cdot 120 - \ 5 \cdot 47 &= 5, \\
-9 \cdot 120 + 23 \cdot 47 &= 1.
\end{aligned}$$

L'esponente cercato è quindi $E = 23$.

3. Sia R la relazione su $\mathbf{N} \times \mathbf{N}$ definita nel modo seguente: si ha che $(n, m)R(n', m')$ se e solo se $n - m = n' - m'$
   (a) Stabilire se R è una relazione di equivalenza;
   (b) In caso affermativo, determinare quante sono le classi di equivalenza e descriverle.

(a) Siccome $n - m = n - m$ per ogni $(n, m) \in \mathbf{N} \times \mathbf{N}$, la relazione è riflessiva. Se $(n, m)R(n', m')$, allora $n - m = n' - m'$ e quindi anche $n' - m' = n - m$ e vale $(n', m')R(n, m)$. La relazione è quindi simmetrica. Finalmente, se $(n, m)R(n', m')$ e $(n', m')R(n'', m'')$ allora si ha che $n - m = n' - m'$ e $n' - m' = n'' - m''$. Questo implica che vale anche $n - m = n'' - m''$ e quindi $(n, m)R(n'', m'')$. Concludiamo che la relazione è transitiva. Si tratta quindi di una relazione di equivalenza.
(b) Due 'punti' (n, m) e (n', m') appartengono alla stessa classe di equivalenza se e solo se le differenze $n - m$ e $n' - m'$ sono uguali. Questa differenza caratterizza quindi la classe di equivalenza. Siccome la differenza può essere un qualsiasi numero in $\mathbf{Z}$, vediamo che le classi di equivalenza corrispondono biettivamente agli elementi di $\mathbf{Z}$. Una biezione è data da

$$\text{"classe di } (n, m)\text{"} \quad \mapsto \quad n - m.$$

4. Siano x, y, z variabili di un algebra di Boole. Trovare un'espressione *minimale* Booleana per $xyz + xy'z + x'yz + x'y'z + x'y'z'$.

Consideriamo i primi due termini dell'espressione E data sopra. Applicando il metodo del 'consenso' e quello dell'assorbimento, abbiamo che $xyz + xy'z = xyz + xy'z + xz = xz$. Similmente, considerando gli ultimi due termini, abbiamo che $x'y'z + x'y'z' = x'y'z + x'y'z' + x'y' = x'y'$. Sostituendo queste due formule nell'espressione E, troviamo

$$E = xz + x'yz + x'y'.$$

Applicando ancora il metodo del consenso e quello dell'assorbimento abbiamo che

$$\begin{aligned} E &= xz + x'yz + yz^2 + x'y', \\ &= xz + x'yz + yz + x'y', \\ &= xz + yz + x'y', \\ &= yz + xz + x'y' + y'z, \\ &= yz + y'z + z + xz + x'y', \\ &= z + x'y'. \end{aligned}$$

Questa espressione è minimale.