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. Sia data la relazione $623 \cdot 30 - 45 \cdot 413 = 105$.
   (i) Dire quale può essere il valore di $mcd(413, 30)$ (per rispondere a questa domanda non è necessario calcolarlo esplicitamente).
   (ii) Determinare tutte le soluzioni intere dell'equazione diofantea

$$623x - 45y = 105.$$

Sol. (i) Per il Teorema di Bezout, il massimo comun divisore $mcd(413, 30)$ deve dividere $105 = 3 \cdot 5 \cdot 7$. Quindi può essere $1, 3, 5, 7, 15, 21, 35, 105$.

(ii) Calcoliamo il massimo comun divisore $mcd(623, 45)$ con l'algoritmo di Euclide:

$623 = 13 \cdot 45 + 38$
$45 = 1 \cdot 38 + 7$
$38 = 5 \cdot 7 + 3$
$7 = 2 \cdot 3 + 1$,
da cui $mcd(623, 45) = 1$. La relazione $623 \cdot 30 - 45 \cdot 413 = 105$ ci dice che una soluzione particolare dell'equazione $623x - 45y = 105$ è data da $(30, -413)$. Ne segue che la soluzione generale dell'equazione $623x - 45y = 105$ è data da

$$(x, y) = (30, 413) + M(45, 623) = (30 + M45, 413 + M623), \qquad M \in \mathbb{Z}.$$

2. Sia X un insieme e sia $\mathcal{P}(X)$ l'insieme delle parti di X. Sia R la relazione su $\mathcal{P}(X)$ così definita: dati A,$B \in \mathcal{P}(X)$,

$$A\,R\,B \quad \Leftrightarrow \quad A \cap B \neq \emptyset.$$

   Determinare se R è o meno riflessiva, simmetrica, antisimmetrica, transitiva (motivare bene le risposte).

Sol.: R non è riflessiva: se $A = \emptyset \in \mathcal{P}(X)$, vale $A \cap A = \emptyset$, per cui A non è in relazione con A.

R è simmetrica: se ARB, cioè $A \cap B \neq \emptyset$, anche $B \cap A \neq \emptyset$, cioè BRA.

R non è antisimmetrica: da ARB, cioè $A \cap B \neq \emptyset$, e BRA, cioè $B \cap A \neq \emptyset$, NON segue che $A = B$. Per esempio sia $X = \{0, 1, 2\}$. Per gli insiemi $A = \{0, 1\}$ e $B = \{0\}$, valgono entrambe le relazioni ARB ed BRA, ma $A \neq B$.

R non è transitiva: ARB, cioè $A \cap B \neq \emptyset$, e BRC, cioè $B \cap C \neq \emptyset$, NON implicano ARC, cioè $A \cap C \neq \emptyset$. Ad esempio sia $X = \{0, 1, 2, 3\}$. Dati $A = \{0, 1\}$, $B = \{1, 2\}$ e $C = \{2, 3\}$ valgono le relazioni ARB e BRC, ma A non è in relazione con C, dato che $A \cap C = \emptyset$.

3. Siano dati $N = 77$ ed $E = 17$.
   (a) Determinare un intero D in modo che la terna $N,\ E,\ D$ formi un kit RSA con chiavi pubbliche N ed E e chiave segreta D.
   (b) Criptare il messaggio $m = 25$ con il kit RSA del punto precedente (impostare il calcolo).
   (c) Decriptare il messaggio criptato $mc = 10$ con il kit RSA del punto precedente (impostare il calcolo).

Sol.: (a) Abbiamo $N = 77 = 7 \cdot 11$, con $p = 7$ e $q = 11$, da cui $(p-1)(q-1) = 6 \cdot 10 = 60$. La chiave D è data da

$$D = E^{-1} \bmod (p-1)(q-1),$$

cioè $D = 17^{-1} \bmod 60$. Dall'algoritmo di Euclide troviamo $mcd(17, 60) = 1$:

$$60 = 3 \cdot 17 + 9, \quad 17 = 1 \cdot 9 + 8, \quad 9 = 1 \cdot 8 + 1$$

e dall'algoritmo di Euclide esteso

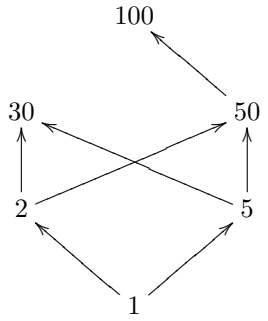
$1 \cdot 60 + 0 \cdot 17 = 60$
$0 \cdot 60 + 1 \cdot 17 = 17$
$1 \cdot 60 + (-3) \cdot 17 = 9$
$-1 \cdot 60 + 4 \cdot 17 = 8$
$2 \cdot 60 + (-7) \cdot 17 = 1$

Da cui $17^{-1} \equiv -7 \equiv 53 \bmod 60$.

4. Sia $A = \{1, 2, 5, 30, 50, 100\}$.
   (a) Disegnare il diagramma di Hasse di $(A, \leq)$, dove $\leq$ è l'ordinamento standard.
   (b) Disegnare il diagramma di Hasse di $(A, \mid)$, dove $\mid$ è l'ordinamento dato dalla "divisibilità" (ossia mRn se $m|n$).
   (c) Determinare l'insieme dei maggioranti e l'insieme dei minoranti di 30 nei casi (a) e (b).

Sol.: (a) In questo caso $(A, \leq)$ è un insieme totalmente ordinato, per cui il diagramma di Hasse risulta un segmento verticale, con gli elementi di A disposti in ordine crescente dal basso in alto.

(b) In questo caso $(A, \leq)$ non è un insieme totalmente ordinato, ed il diagramma di Hasse è dato da



(c) Nel caso (a) abbiamo $min(30) = \{1, 2, 5, 30\}$ e $magg(30) = \{30, 50, 100\}$.
Nel caso (b) abbiamo $min(30) = \{1, 2, 5, 30\}$ e $magg(30) = \{30\}$.

5. Mediante quantificatori e connettivi logici, esprimere i seguenti enunciati definiti sugli interi $\mathbb{Z}$:
   (a) Il prodotto di due interi negativi è positivo.
   (b) La differenza di due interi negativi non è necessariamente negativa.
   (c) La media aritmetica di due interi positivi è positiva.

Sol.: $\forall m < 0\ \forall n < 0 \quad m \cdot n > 0$;
$\exists n < 0\ \exists m < 0 \quad m - n \geq 0$;
$\forall m > 0\ \forall n > 0 \quad \frac{1}{2}(m + n) > 0$;

6. In un'algebra di Boole $(A, +, \cdot, ')$, siano date le espressioni

$$E: \quad xy'z + y'z' + xy'z', \qquad F: \quad xyz + x'y + xz.$$

(a) determinare se E ed F sono equivalenti;
(b) scrivere E come somma di implicanti primi;
(c) determinare una forma minimale di E.

Sol.: (a) & (b) Portiamo entrambe le espressioni nella forma *somma di tutti gli implicanti primi.* Poiché tale forma è unica, ci dirà se E ed F sono o meno equivalenti, ed avremo risposto anche alla domanda (b). Applicando le proprietà delle operazioni di $(A, +, \cdot, ')$ troviamo

$$E: \quad xy'z + y'z' + xy'z' \;=\; xy'(z + z') + y'z' \;=\; xy' + y'z'.$$

Poiché il metodo del consenso non ha passi non banali, quella che abbiamo trovato è la somma di tutti gli implicanti primi di E.
Similmente

$$F: \quad xyz + x'y + xz \;=\; xz(y + 1) + x'y \;=\; xz + x'y \;=\; xz + x'y + zy,$$

dove l'ultima uguaglianza è stata ottenuta sommando zy, che è il consenso tra xz e $x'y$. Poiché il metodo del consenso non ha passi non banali, quella che abbiamo trovato è la somma di tutti gli implicanti primi di F.
Ne segue che E ed F non sono equivalenti.
(c) Per determinare una forma minimale di E, completiamo $xy' + y'z'$:

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

Poiché i due addendi sono distinti, nessuno dei due può essere eliminato. Dunque $xy' + y'z'$ è una forma minimale di E.