

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.

$$1. \text{ Siano dati i sistemi di congruenze } \begin{cases} x \equiv 5 \pmod{6} \\ 5x \equiv 1 \pmod{4} \end{cases} \quad e \quad \begin{cases} 3x \equiv 5 \pmod{6} \\ x \equiv 1 \pmod{4} \end{cases}$$

(i) Determinare quale dei due ha soluzioni intere, spiegando la risposta.

(ii) Determinare tutte le soluzioni intere di tale sistema.

Sol. (i) Il secondo sistema non ha soluzioni intere. Infatti $\text{mcd}(3,6) = 3$ e 3 non divide 5, quindi già la prima equazione del sistema è incompatibile. Il secondo sistema invece ammette soluzioni intere. Poiché $\text{mcd}(1,6) = 1|5$ e $\text{mcd}(5,4) = 1|1$ le due equazioni ammettono singolarmente soluzioni intere. Inoltre $\text{mcd}(4,6) = 2$ divide $1 - 5 = -4$, e questo garantisce l'esistenza di soluzioni intere per il sistema.

(ii) Osserviamo che la seconda equazione è equivalente a $x \equiv 1 \pmod{4}$. Sostituendo le soluzioni della prima equazione $x = 5 + 6k$, $k \in \mathbb{Z}$ nella seconda, troviamo l'equazione diofantea

$$5 + 6k = 1 + 4h \quad \Leftrightarrow \quad 6k + 4h = -4.$$

Una soluzione particolare è data da $(k, h) = (-4, 5)$. Le soluzioni dell'equazione omogenea associata sono date da $(2M, -3M)$, $M \in \mathbb{Z}$ (notare che l'equazione omogenea associata è equivalente a $3k + 2h = 0$!!!). Quindi per $k = -4 + 2M$, troviamo che le soluzioni intere del sistema sono date da

$$x = 5 + 6(-4 + 2M) = 5 - 24 + 12M = -19 + 12M = 5 + 12M, \quad M \in \mathbb{Z}.$$

2. Sia X un insieme. Si definisca su $\mathcal{P}(X)$ la seguente relazione: $A R B$ se $|A| = |B|$ oppure $|A| = |B^c|$ (qui $|A|$ indica la cardinalità di A e A^c il complementare di A in X).

(a) Verificare che si tratta di una relazione di equivalenza.

(b) Determinare le classi di equivalenza di $\mathcal{P}(X)$, se $X = \{a, b, c, d, e, f, g, h\}$.*Sol.* (a) La relazione è riflessiva: $|A| = |A|$, per ogni $A \in \mathcal{P}(X)$;La relazione è simmetrica: se $|A| = |B|$ allora $|B| = |A|$; se $|A| = |B^c|$ allora $|B| = |A^c|$;

La relazione è transitiva: dobbiamo esaminare le varie possibilità.

Se $|A| = |B|$ e $|B| = |C|$ allora $|A| = |C|$; $|A| = |B|$ e $|B| = |C^c|$ allora $|A| = |C^c|$;se $|A| = |B^c|$ e $|B^c| = |C|$ allora $|A| = |C|$;se $|A| = |B^c|$ e $|B^c| = |C^c|$ allora $|A| = |C^c|$.

(b) La cardinalità di X è 8. Le classi di equivalenza contengono tutti gli insiemi A della stessa cardinalità e quelli di cardinalità $8 - \text{card}(A)$: in totale sono 5 e sono parametrizzate dalle coppie di numeri $(0, 8)$, $(1, 7)$, $(2, 6)$, $(3, 5)$, $(4, 4)$.

La classe $(0, 8)$ contiene l'insieme vuoto e l'intero insieme X ; la classe $(1, 7)$ contiene tutti gli insiemi di cardinalità 1 e di cardinalità 7, etc....

3. Il signor Rossi desidera ricevere messaggi criptati e adotta il criptosistema RSA.

(a) Preparare per il signor Rossi un kit di chiavi pubbliche N , E e chiave segreta D , con $N = 51$ e $D = 7$.(b) Il signor Rossi riceve il messaggio criptato $m = 13$. Lo decripta con la sua chiave segreta. Cosa trova?(c) Vogliamo inviare al signor Rossi il messaggio $m = 19$ e lo criptiamo. Che cosa gli inviamo?

Sol. (a) La chiave pubblica $N = 51$ è il prodotto dei primi $p = 3$ e $q = 17$. La chiave mancante E è data dall'inverso di D modulo $(p-1)(q-1) = 2 \cdot 16 = 32$:

$$E \equiv D^{-1} \equiv 23 \pmod{32}.$$

(b) Rossi calcola

$$m^D \equiv 13^7 \equiv 4 \pmod{51}.$$

Dunque il messaggio decriptato è 4.

(c) Il messaggio criptato che spediamo a Rossi è

$$m^E \equiv 19^{23} \equiv 43 \pmod{51}.$$

4. Si consideri il reticolo (D_{30}, mcd, mcm) .

(a) Verificare che $6 \in D_{30}$ e determinare $\{x \in D_{30} \mid x \leq 6\}$, dove " \leq " è la relazione di ordine parziale indotta su D_{30} dalle operazioni di reticolo.

(b) Determinare limite inferiore e limite superiore di D_{30} .

(c) Determinare se D_{30} è un reticolo complementato e se il complemento è unico (per ogni elemento di D_{30} esibire un eventuale complemento).

Sol. (a) Abbiamo che $30 = 2 \cdot 3 \cdot 5$ e il reticolo dei divisori di 30 è dato da

$$D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}.$$

In particolare $6 \in D_{30}$. La relazione di ordine parziale indotta dalle operazioni di reticolo è data da $a \leq b$ se $mcd(a, b) = a$, e ciò equivale a richiedere che a divide b : $a \mid b$. L'insieme $\{x \in D_{30} \mid x \leq 6\}$ coincide con l'insieme dei divisori di 6: $\{1, 2, 3, 6\}$.

(b) Il limite inferiore di D_{30} è 1: infatti $mcd(1, a) = 1$, per ogni $a \in D_{30}$;

Il limite superiore di D_{30} è 30: infatti $mcd(a, 30) = a$, per ogni $a \in D_{30}$.

(Vedi anche il diagramma di Hasse che è un "cubo" sospeso per uno dei vertici)

(c) Poiché 30 è il prodotto di tre primi distinti, D_{30} è un reticolo booleano: è limitato, distributivo e complementato. Ne segue che il complemento di ogni elemento è unico: $\bar{a} = \frac{30}{a}$.

Si verifica infatti che $mcd(a, \frac{30}{a}) = 1$ e $mcm(a, \frac{30}{a}) = 30$.

Nel nostro caso abbiamo: $\bar{1} = 30$, $\bar{2} = 15$, $\bar{3} = 10$, $\bar{5} = 6$.

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

$$E : xz + xy'z' + xyz' \qquad F : xyz + x'z + yz'.$$

(a) Determinare se E ed F sono equivalenti;

(b) Determinare se E è somma di implicanti primi;

(c) Determinare se E è in forma minimale.

Sol. (a) Passando alla forma normale disgiuntiva (che è unica) delle due espressioni, troviamo rispettivamente

$$E \sim xyz + xy'z + xy'z' + xyz', \qquad F \sim xyz + x'yz + x'y'z + xyz' + x'yz'.$$

Poiché le espressioni trovate sono diverse, E ed F non sono equivalenti.

(b) Poiché si possono applicare dei passi non banali del metodo del consenso ad F , possiamo subito concludere che $F : xyz + x'z + yz'$ non è somma di implicanti primi.

(c) In particolare $F : xyz + x'z + yz'$ non è in forma minimale (ogni forma minimale è somma di implicanti primi).

Applicando il metodo del consenso ad $F : xyz + x'z + yz'$, troviamo:

$$Q_{12} = yz, \qquad F + Q_{12} = xyz + x'z + yz' + yz = x'z + yz' + yz = x'z + (z + z')y = x'z + y.$$

Dunque $x'z + y$ è somma di tutti gli implicanti primi di F .

Completando i due termini, troviamo

$$x'z(y + y') = x'yz + x'y'z, \qquad (x + x')(z + z')y = xyz + xyz' + x'yz + x'y'z'.$$

Poiché nessuna dei due è "contenuto" nell'altro, abbiamo che $x'z + y$ è anche una forma minimale.

6. Sia $f: \mathbb{R} \rightarrow \mathbb{R}$ la funzione data da $f(t) = e^t$. Considerare il seguente enunciato

$$P(t) : \quad \forall y \in]0, +\infty[\quad \exists t \in \mathbb{R} : f(t) = y \wedge t > 0.$$

(a) Determinare se $P(t)$ è vero;

(b) Determinare la negazione di $P(t)$ (non ci devono essere negazioni davanti ad un quantificatore o davanti ad un'espressione contenente connettivi logici).

Sol. (a) In parole povere $P(t)$ dice che la funzione esponenziale ristretta ai reali positivi $\exp :]0, +\infty[\rightarrow]0, +\infty[$ è suriettiva. Questo è falso: infatti la funzione esponenziale non assume nessun valore $y \in]0, 1]$ sui reali positivi.

(b) La negazione di $P(t)$ è la seguente:

$$\neg P(t) : \quad \exists y \in]0, +\infty[\quad \forall t \in \mathbb{R} : f(t) \neq y \vee t \leq 0.$$