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. *Sia* $A = \{x = 4 + 7m,\ m \in \mathbb{Z}\}$ *e sia* B *l'insieme di tutte le soluzioni intere della congruenza* $3x \equiv 5 \bmod 14$.
   (a) Determinare B.
   (b) Determinare se $A = B$, *se* $A \subset B$, *se* $B \subset A$ *oppure se non vale nessuna delle tre, giustificando bene la risposta.*

2. *Sia dato il seguente enunciato:*

$$\Big((p \in \mathbb{N}) \bigwedge (p \text{ primo})\Big) \quad \Rightarrow \quad \Big(\Big((a \in \mathbb{Z}) \bigwedge (\mathrm{mcd}(a,p) = 1)\Big) \Rightarrow \big(a^{p-1} \equiv 1 \bmod p\big)\Big). \qquad (*)$$

   (a) Cosa dice l'enunciato? È vero?
   (b) Usare l'enunciato $(*)$ *per dimostrare che* 6 *non è primo.*
   (c) Calcolare $5^{111} \bmod 6$.

3. *Sia* p *un numero primo e sia* $\mathbb{Z}_{p^2}^*$ *il gruppo delle classi resto modulo* p^2 *che hanno inverso moltiplicativo.*
   (a) Quanti elementi ha $\mathbb{Z}_{p^2}^*$*? (spiegare bene la risposta).*
   (b) Date le classi resto $\overline{10},\ \overline{5},\ \overline{9} \in \mathbb{Z}_{100}$, *determinare quali fra esse appartengono a* $\mathbb{Z}_{100}^*$. *Quando esiste, determinarne l'inverso moltiplicativo (giustificare bene le risposte).*
   (c) Calcolare $\overline{7}^{152} \cdot \overline{4}^{13} + \overline{2}^{17}$ *in* $\mathbb{Z}_{11}$.

4. *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 $A, B \in \mathcal{P}(X)$, diciamo che $A \ R \ B$ se $A \cup B = A$. Determinare se la relazione R è riflessiva, simmetrica, antisimmetrica o transitiva (per ognuna di queste proprietà, verificare che vale oppure esibire almeno una coppia A, B per cui non vale).*

5. *Sia dato l'insieme $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, ordinato mediante la divisibilità.*
   (a) Disegnare il diagramma di Hasse di A. Determinare l'insieme dei maggioranti e l'insieme dei minoranti di $S = \{2, 3\} \subset A$;
   (b) Richiamare la definizione di reticolo;
   (c) Determinare se $(A, \mid)$ è o meno un reticolo, giustificando la risposta.

6. *Il signor Rossi desidera ricevere messaggi criptati e decide di adottare il criptosistema RSA.*
   (a) La ditta gli fornisce un kit con chiavi pubbliche $N = 91 = 7 \cdot 13$ ed $E = 23$ e chiave segreta $D = 47$. Vanno bene? (spiegare).
   (b) Preparare un kit di chiavi pubbliche N', E' e chiave segreta D' per il signor Bianchi, con $N' = 91$ ed $E' = 11$.
   (c) Il signor Verdi, che ha chiavi pubbliche $N = 77$ ed $E = 13$ e chiave privata $D = 37$, riceve il messaggio criptato $m = 13$. Decriptarlo.