

Cognome e Nome: _____.

Data: _____.

ISTRUZIONI. Riportare le soluzioni in bella copia. La soluzione deve essere leggibile, corretta, completa e sintetica.

I risultati appariranno nella pagina web del docente la settimana prossima.

1. Enunciare e dimostrare il Teorema di Lagrange.
2. Dare la definizione di gruppo ciclico ed enunciare il Teorema di classificazione dei gruppi ciclici. Dare un esempio significativo di gruppo ciclico.
3. Determinare le soluzioni del sistema di congruenze

$$\begin{cases} 3x \equiv 15 \pmod{21} \\ 44x \equiv 20 \pmod{12} \\ 6x \equiv 21 \pmod{15} \end{cases}$$

4. Spiegare come costruire un campo con 27 elementi.
5. Usando la parola chiave $\mathbf{k} = \text{CIFRATO}$ crittare la frase CHI DORME NON PIGLIA PESCI (cifrario di Vigenère).
6. Crittare il messaggio SO usando il metodo RSA con chiave (2537, 13).
7. Sia C il codice ternario lineare con matrice generatrice

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

Elencarne le parole, determinare la distanza minima. Dedurre che C è un codice perfetto.

8. Risolvere la ricorrenza $x_0 = 2, x_1 = 1, x_n = x_{n-1} + x_{n-2}$.
9. Sia $F_0 = 0, F_1 = 1$, e per $n \geq 2, F_n = F_{n-1} + F_{n-2}$ la successione di Fibonacci. Trovare e dimostrare una formula per $F_0^2 + F_1^2 + \dots + F_n^2$. (Suggerimento: potrebbe essere utile guardare la fattorizzazione del risultato).
10. Assegnati gli insiemi

$$A_1 = \{\dots, -4, -3, -2, -1, 0\}$$

$$A_2 = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

$$A_3 = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$$

$$A_4 = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$$

$$A_5 = \{\dots, -6, -3, 0, 3, 6, \dots\}$$

Disegnare il grafo che ha un vertice per ciascuno di questi insiemi ed uno spigolo che collega due vertici se due insiemi hanno intersezione non vuota. Il grafo è connesso? Quali sono i gradi dei vari vertici? Scrivere la matrice di adiacenza e quella di incidenza. È possibile trovare un circuito euleriano? Un cammino euleriano?