Risolvere il massimo numero di esercizi accompagnando le risposte con spiegazioni chiare ed essenziali. Inserire le risposte negli spazi predisposti. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Scrivere il proprio nome anche nell'ultima pagina. 1 Esercizio = 4 punti. Tempo previsto: 2 ore. Nessuna domanda durante la prima ora e durante gli ultimi 20 minuti.

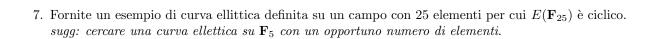
FIRMA	1	2	3	4	5	6	7	8	TOT

1. Dimostrare che ogni elemento di $\mathbf{F}_{p^{\alpha}}$ ammette esattamente una radice p-esima. Calcolare la radice quadrata di $\alpha \in \mathbf{F}_2[\alpha], \alpha^5 = \alpha^2 + 1$ assumendo che $X^5 + X^2 + 1$ è irriducibile su \mathbf{F}_2 .

2. Dopo aver spiegato il funzionamento dei sistemi crittografici che usano i logaritmi discreti, si illustri il funzionamento dello scambio chiavi Diffie Hellmann utilizzando come gruppo \mathbf{F}_{16}^* .

3. Descrivere in dettagli l'Algoritmo Baby Steps Giant Steps per il calcolo dei logaritmi discreti.
4. Siano n e m interi tali che 5 n m, $5n \equiv 3 \mod 8m$ e $m \equiv 13 \mod 60$. Calcolare il simbolo di Jacobi n giustificando ogni passaggio.





8. Sia $E: y^2 = x^3 - 5x + 8$ e siano $P = (10,7), Q = (3,11) \in E(\mathbf{F}_{101})$. Calcolare 2P e P + Q. Sapendo che il punto $R = (1,2) \in E(\mathbf{F}_{101})$ ha ordine 31, cosa possiamo dire della struttura di $E(\mathbf{F}_{101})$?