COGNOME .... *NOME* .... *MATRICOLA* ....

Risolvere gli esercizi accompagnando le risposte con spiegazioni chiare ed essenziali. *Inserire le risposte negli spazi predisposti. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI.* Ogni esercizio vale 7.5 punti.

1.
   a. Dire quanti sono i polinomi monici irriducibili di grado 2 sul campo $\mathbf{F}_7$.
   b. Dire quanti sono i polinomi primitivi di grado 2 sul campo $\mathbf{F}_7$.
   c. Stabilire la probabilità che un polinomio irriducibile di grado 2 sul campo $\mathbf{F}_7$ sia primitivo.
   d. Scrivere un polinomio primitivo e un polinomio irriducibile ma non primitivo.

2. Supponiamo che Antognoni e Bettega vogliano scambiarsi una chiave utilizzando l'algoritmo Diffie-Hellmann sul campo $\mathbf{F}_{53}$.
   a. Trovare il più piccolo elemento primitivo in $\mathbf{F}_{53}^*$.
   b. Usando tale elemento primitivo, scegliere gli altri parametri dell'algoritmo e determinare la corrispondente chiave DH.

3. Fattorizzare il polinomio $f(x) \in \mathbf{F}_7[x]$ definito come $f(x) = (x^{21} + x^7 + 3)(x^2 + 1)$. Determinare quanti elementi ha il campo di spezzamento $\mathbf{L}$ di $f(x)$. Scrivere un polinomio irriducibile $g(x) \in \mathbf{F}_7[x]$ tale che, indicando con α una radice di $g(x)$, si abbia $\mathbf{L} \simeq \mathbf{F}_7(\alpha)$.

---

4. Scrivere una formula che esprima, in funzione di p, il numero $\mathbf{I}_6(p)$ dei polinomi irriducibili di grado 6. Inoltre, se p è un numero primo dispari tale che $p - 1 = 6l$ e $p + 1 = 4r$, con l e r due primi dispari, determinare il numero $\mathbf{P}_2(p)$ dei polinomi primitivi di grado 2 in $\mathbf{F}_p[x]$, in funzione di p.
