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

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 = 3 punti. Tempo previsto: 2 ore. Nessuna domanda durante la prima ora e durante gli ultimi 20 minuti.

1. Definire il concetto di curva ellittica su un campo finito ed il gruppo di Mordell-Weyll associato.

2. Consideriamo la curva $y^2 = x^3 + x + 6$ sul campo $\mathbf{F}_7$. Descrivere $E(\mathbf{F}_7)$.

3. Descrivere l'algoritmo dello scambio delle chiavi di Diffie-Helmann sulle curve ellittiche.

4. Sia g una radice primitiva di $\mathbf{F}_p$. Dimostrare le seguenti proprietà del logaritmo discreto:
$$\log_g(a \cdot b) = \log_g(a) + \log_g(b), \qquad \log_g(a^n) = n \log_g(a) \qquad (\bmod\ p-1).$$

5. Consideriamo il campo base $\mathbf{F}_5$. Determinare il numero dei polinomi monici irriducibili di grado 12. Qual è la probabilità che, preso random un polinomio monico di grado 12, esso sia irriducibile?

6. Consideriamo il polinomio $f = x^3 + x + 1 \in \mathbf{F}_5[x]$. Dopo aver verificato che è irriducibile, trovare una radice primitiva per il campo:

$$\mathbf{F}_5[x]/(f) \; = \{a + b\theta + c\theta^2 \mid \theta^3 = -\theta - 1\}.$$

7. Calcolare il $\log_3(13)$ nel campo $\mathbf{F}_{31}$, utilizzando un qualsiasi metodo.

8. Dimostrare che il polinomio $x^2 + 1$ è irriducibile su tutti i campi finiti $\mathbf{F}_p$ con $p \equiv 3 \pmod 4$.

9. Si descrivino tutti i valori di $a \in \mathbf{F}_p$ per cui il polinomio: $f(x) = x^2 + a$ è irriducibile, e si dimostri che tale polinomio non può mai essere primitivo.

10. Mostrare che tutti i polinomi del tipo $x^p + x + 1$ sono riducibili su $\mathbf{F}_p$, con $p \geq 3$.

11. Dopo aver scritto tutti i polinomi irriducibili di grado ≤ 4 su $\mathbf{F}_2$, mostrare che il polinomio $f(x) = x^5 + x^2 + 1$ è irriducibile.

12. Descrivere tutti i sottocampi di $\mathbf{F}_{5^{30}}$.

NOME E COGNOME	1	2	3	4	5	6	7	8	9	10	11	12	TOT.
....													