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. Scrivere il proprio nome anche nell'ultima pagina.* Ogni esercizio vale 3 punti.

1. Si stimi il numero di operazioni bit necessarie a calcolare la derivata di un polinomio di grado n^2 in cui tutti i coefficienti sono minori di n.

2. Si risolva il seguente sistema di equazioni di congruenze

$$\begin{cases} x^3 \equiv 1 \bmod 7 \\ x^2 \equiv 1 \bmod 5 \end{cases}.$$

3. Quale è la probabilità che un polinomio irriducibile f di grado 8 su $\mathbf{F}_7$ risulti primitivo?

4. Si illustri la nozione di pseudo primo di eulero e si indichi la sua applicazione in crittografia.

5. Fattorizzare $f(x) = (x^{10} + 3x^5 + 1)(x^2 + 2)(x^2 + 1)$ su $\mathbf{F}_5$ e dopo aver fissato un campo di spezzamento $\mathbf{F}$ per f, si scrivano tutte le radici di $f(x)$ in $\mathbf{F}$.

6. Spiegare il funzionamento del metodo dello scambio delle chiavi Diffie–Hellman sul gruppo dei punti razionali di una curva ellittica.

7. Dopo aver verificato che si tratta di una curva ellittica, determinare l'ordine e la struttura del gruppo dei punti razionali della curva ellittica su $\mathbf{F}_7$

$$y^2 = x^3 - x + 5.$$

8. Si calcoli il seguente simbolo di Jacobi: $\left(\frac{234564}{134431}\right)$.

9. Scrivere in una sola riga il codice (in PARI) per ottenere:
   a Numero di cifre binarie di x;
   b L' inverso aritmetico di $a \in (\mathbf{Z}/n\mathbf{Z})^*$;
   c Un primo con al massimo m cifre binarie.

10. Scrivere un programma in PARI per ottenere un vettore contenente i numeri minori di 10^{20} che sono pseudoprimi forti, per almeno una base random.

NOME E COGNOME	1	2	3	4	5	6	7	8	9	10	TOTALE
.....											